2025–2026

CYBERAUSTRALIA

AISA Australian Cyber Conference

ECU
EDITH COWAN UNIVERSITY

Stay one step ahead with Australia's only International Cyber Security Centre of Excellence.

With our reliance on internet-based technology, there's never been a greater need to protect Australian businesses, government and the community.

ECU offers the largest academic cyber security and research program in Australia. Our undergraduate and postgraduate courses are designed to address the needs of industry for cyber security professionals within government, law enforcement and industry.

We are the first and only university from Australia to join the International Cyber Security Centre of Excellence as an Affiliate Member. This organisation was initiated in 2019 by universities across UK, Europe, the US and Japan and acts as a hub for cyber security research, education and advocacy.

ECU's School of Science offers world-class research in Critical Infrastructure, Emerging Technologies and Human Factors in Security and has a history of delivering successful research projects for State, Federal and Defence agencies.

Creative thinkers made here.

For more information

ECU.EDU.AU/CYBER-SECURITY

FOREWORD

Scarlett McDermott,
Director,
Australian Information
Security Association

Scarlett McDermott

Public discourse about cyber security has been growing and evolving over recent years. No longer simply a topic for security teams in large enterprises, cyber security vernacular is now popping up everywhere – from dining tables, to boardrooms around the country.

While this general awareness of cyber risks and online safety measures is overwhelmingly positive, it does raise interesting considerations for our industry. During my first year on the board of the Australian Information Security Association (AISA), I've been reflecting on the conversations we have about cyber security at all levels, how they represent us as an industry, and what they might mean for the road ahead.

Cyber security conversations around the dinner table or barbecue have become commonplace. Unfortunately, this is not caused by a national love of information security, but instead due to the proliferating impact of cybercrime in Australian society. Between high-profile breaches and routine scam campaigns, you would be hard-pressed to find anyone in Australia with more than two degrees of separation from the impacts of cybercrime or privacy breaches. You can see the impact in everyday behaviour – gone are the days when most people would answer the phone to an unknown number!

Recently, I've observed a troubling trend of complacency in these casual chats – the feeling that it's all out there already anyway when a breach occurs. Between direct impacts of cybercrime and – perhaps even more insidious – challenges related to data privacy when dealing with corporations or even political parties, we're at a critical juncture when it comes to public trust in technology. As cyber professionals, these 'off duty' conversations can be an important grassroots way to build trust and help others to take action. By knowing the practical steps others can take, and which resources to guide them to, we can help others to move past apathy and towards action.

Beyond the dinner table, cyber security discussions have flooded into workplaces and business events. There's hardly a conference without a panel discussion or presentation on cyber security (often featuring one of our AISA members!). This moment in the spotlight is unusual for what can be a difficult topic for audiences. It's a wonderful opportunity for our industry to speak on the actions needed to build resilience, and we certainly shouldn't squander it thinking that it may last forever.

So, how can we make sure we have a clear and lasting impact in these conversations? For some audience members at these events, this may be their primary interaction with a cyber security professional. It is critical that we recognise that in these moments, we're not just speaking on behalf of ourselves or our employers, but as representatives of our profession. It lends weight to our words, but also comes with a responsibility to ensure that the things we say are accurate, understandable and actionable for our audience.

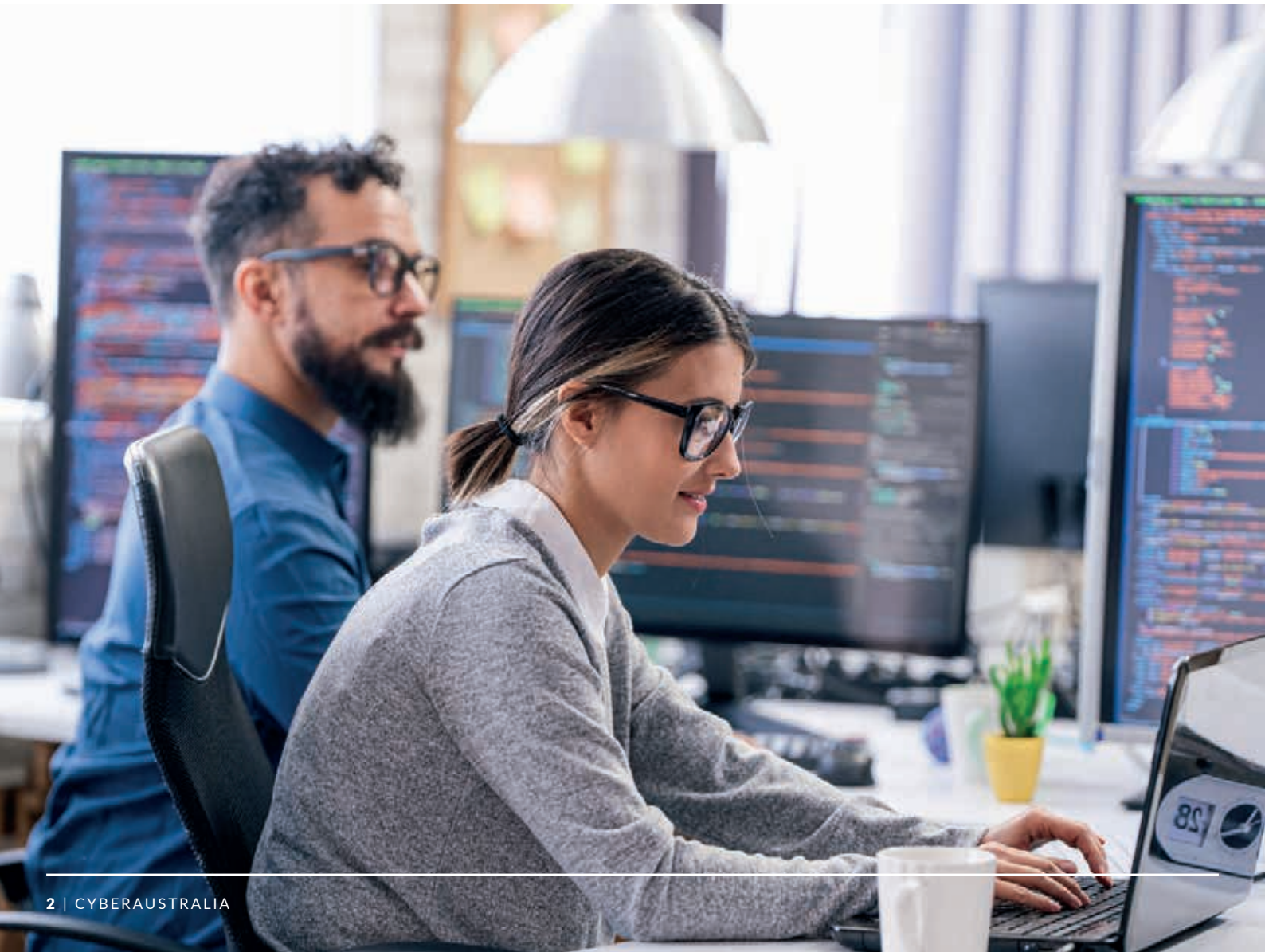
Another arena in which people are increasingly talking about cyber is the boardroom. With directors becoming more aware of technology risk, cyber security leaders are capitalising on an opportunity to reframe cyber from a 'cost of doing business' to a

strategic advantage. These conversations are moving out of the realm of compliance and siloed efforts, and into the realm of business and transformation. The case for integrating security throughout technology and business processes to build resilience has never been stronger. As cyber leaders, we have to speak the language of business in these exchanges to advocate for the safety of staff, end users and others impacted by the technologies we use, as well as for the health of the business.

As regulations shift and the wheels begin to turn on enforcement actions related to cyber negligence, there's a risk of these conversations shifting to protectionism – an approach to cyber security fuelled by risk of personal liability risks taking a short-term or reactive view of a complex, long-term challenge. Cyber leaders are at a pivotal moment where careful use of language and influence will be critical in staying the course. Decisions made on cyber now will have long-lasting impacts.

The impact of technology on society has seldom been more prevalent than it is right now as we work through the paradigm shift of artificial intelligence. The discussions that we have about technology shape more than just expectations – they shape the development, implementation and future of technology. Flowing out of all of them – from the backyard barbecue to the boardroom – comes a national narrative. This is the narrative that shapes attitudes and actions at every level; it's the difference between apathy and engagement. While it can feel like shaping such a big idea is out of reach, remember that each conversation we have about cyber security builds to become that narrative, and each one of us is shaping it every day.

I want to thank all of those AISA members and friends who have generously contributed their own voices here in *Cyber Australia*, and at the Australian Cyber Conference 2025. It has never been more important for our industry to share well-reasoned, thought-provoking perspectives in the service of building our collective cyber resilience. I encourage you to engage with the content here thoughtfully, and continue to grow the national conversation on cyber security in your responses to it. •



CONTENTS

CYBERAUSTRALIA

PUBLISHED BY:

EXECUTIVE MEDIA
NEW YORK | MELBOURNE | ADELAIDE | AUCKLAND

ABN 30 007 224 204

PO Box 256
North Melbourne, VIC, 3051

Tel: 03 9274 4200

Email: media@executivemedia.com.au
Web: www.executivemedia.com.au

PUBLISHER
David Haratsis
david.haratsis@executivemedia.com.au

EDITOR IN CHIEF
Giulia Heppell
giulia.heppell@executivemedia.com.au

CO-EDITOR
Craig Ford

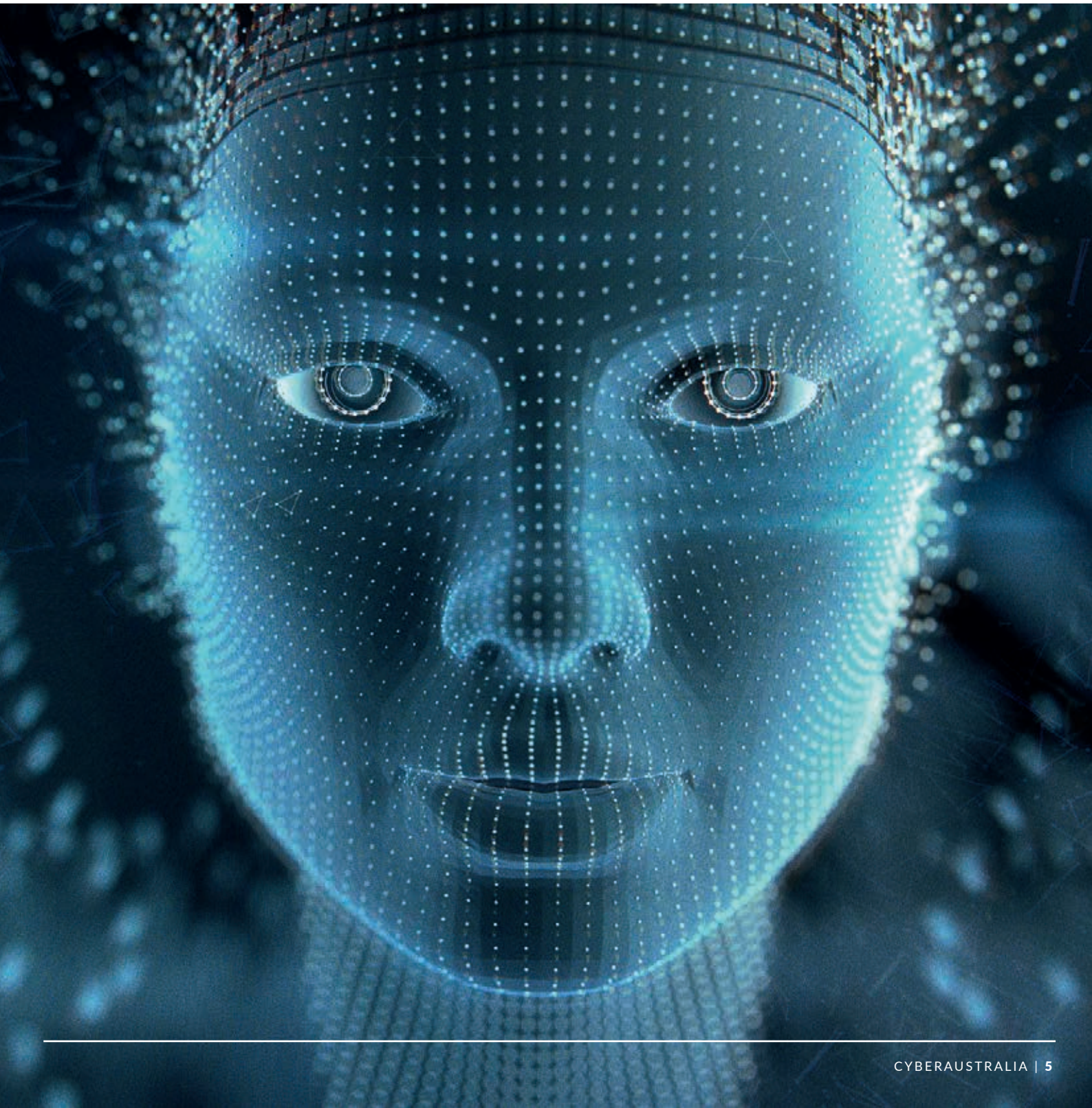
EDITORIAL AND DESIGN TEAM
Eden Cox, Sam Garland and Ruby O'Brien

To continue receiving free cybersecurity publications from Executive Media, scan the QR code.

HELLO, MY NAME IS MACHINE

BY ABBAS KUDRATI, CHIEF IDENTITY SECURITY ADVISOR, SILVERFORT

Demystifying machine identity in a digital world.



Abbas Kudrati

Imagine walking into a party where two guests are wearing the same costume, using the same name tag and ordering the same drink. It's confusing – who's who?

Now, replace those guests with virtual machines in your IT environment. That confusion – distinguishing between systems, knowing which one did what, and assigning accountability – is at the heart of the modern identity crisis in machine identity and access management (IAM).

In our increasingly digital world, machines – not just humans – authenticate, authorise and interact across complex networks. Machines initiate processes, run workloads, access sensitive data and even communicate with other machines. And like humans, these non-human identities (NHIs) need to prove who they are and what they're allowed to do.

Yet, many organisations conflate or misunderstand key identity concepts: identity, credential, identifier and account. Let's unravel these terms and explore how modern IAM can be reimagined.

IDENTITY VERSUS ACCOUNT: NOT THE SAME PARTY GUEST

The most common confusion lies in how we define 'identity' versus 'account'.

An identity is the logical principal authorised to act within a system. It includes:

- unique identifiers (UIDs) (e.g., container ID, instance ID)
- entitlements (what the machine is allowed to do)
- policies and conditions (contextual access rules).

An account, on the other hand, is the formal record of an identity in a particular system. One identity can have multiple accounts across systems – just like a person may have memberships at different organisations.

Scenario:

Consider two cloned virtual machines, identical in configuration but executing different tasks. If they share the same system account without proper session binding or ephemeral credentials, you lose the ability to attribute actions accurately. It's like having identical twins log into your systems under the same name – if something goes wrong, who do you hold responsible?

WHAT MAKES UP A MACHINE IDENTITY?

A machine identity is more than just a UID or a label. It is composed of identifiers, attributes, and policies and entitlements:

- **Identifiers:** Unique traits that distinguish one machine from another (e.g., container ID, cryptographic hash, node location).
- **Attributes:** Descriptive characteristics (e.g., environment, role, version) that provide context, but may not be unique.
- **Policies and entitlements:** Rules defining what the machine can access and under what conditions.

Key clarification:

- All identifiers are attributes, but not all attributes are identifiers.
- Identity does not equal UID – a UID is just one part; identity encompasses who the machine is and what it's allowed to do.

CREDENTIALS: THE PROOF OF IDENTITY

Once a machine declares its identity, it must prove it. That's where credentials come in.

Credentials are the digital proof points – analogous to passports or access cards. They include:

- short-lived tokens (JWTs, OAuth, AWS STS)
- digital certificates
- SAML assertions
- Kerberos tickets (indicating prior authentication).

Modern best practice:

- Ephemeral credentials (bound to workload context) reduce risk.
- Static, shared credentials (e.g., hardcoded passwords) are the real security pitfall – not shared identities themselves.

The pitfall: Static credentials and poor identity binding.

Revisiting our party analogy – if multiple machines share the same static credentials, they all wear the same name tag. This creates:

- security risks (lateral movement if compromised)
- operational blind spots (who did what?).

Real-world example:

A DevOps engineer clones a virtual machine and reuses the same static service account. Now, multiple machines operate under the same persona. When an incident occurs, forensics becomes guesswork.

Solution:

- Dynamic credential binding (e.g., workload identity federation).
- Session isolation (each machine gets unique, short-lived access).

INTRODUCING NHIS: BEYOND JUST MACHINES

An NHI refers to any digital actor not tied to a person. This includes, but is not limited to, machine identities. NHIs represent a broader category of autonomous or automated entities.

Examples of NHIs:

- virtual machines and containers
- service accounts (with proper credential binding)
- application programming interface integrations
- continuous integration and continuous delivery/deployment pipeline jobs
- cloud-native functions (AWS Lambda, Azure Logic Apps).

Clarification:

- All machine identities are NHIs, but not all NHIs are machine identities.
- NHIs also include software-based actors (e.g., scripts, automation workflows).

THE NHI EXPLOSION – BY THE NUMBERS

Insights from Silverfort's latest field research reveal the scale and risk posed by NHIs:

- 80 per cent of security breaches involve compromised NHIs
- NHIs outnumber human identities in many enterprises by 40:1
- 94 per cent of NHIs are not actively monitored
- 83 per cent have no assigned owner
- 34 per cent are stale or dormant for more than 180 days
- 60 per cent have never had credentials rotated
- 70 per cent were created by third-party vendors.

These statistics paint a clear picture: organisations are surrounded by thousands of unmanaged, invisible identities that they cannot secure.

THE FUTURE: EPHEMERAL CREDENTIALS AND IDENTITY-CENTRIC SECURITY

The breakthrough is shifting from static accounts to identity-centric security.

- **Eliminate long-lived credentials:** Use short-lived, workload-bound tokens.
- **Continuous discovery and inventory:** Track NHIs in real time.
- **Least-privilege policies:** Enforce access based on identity context.
- **Behavioural monitoring:** Detect anomalies and auto-revoke if compromised.

This is not 'accountless' identity; there's always an identity and trust policy. The shift is towards ephemeral credentials bound to workload context, reducing attack surfaces.

FINAL THOUGHTS: EVERY MACHINE – AND SCRIPT – DESERVES A SECURE IDENTITY

In today's enterprise, identities don't just belong to people; they belong to the machines, scripts, and workloads that power your digital business.

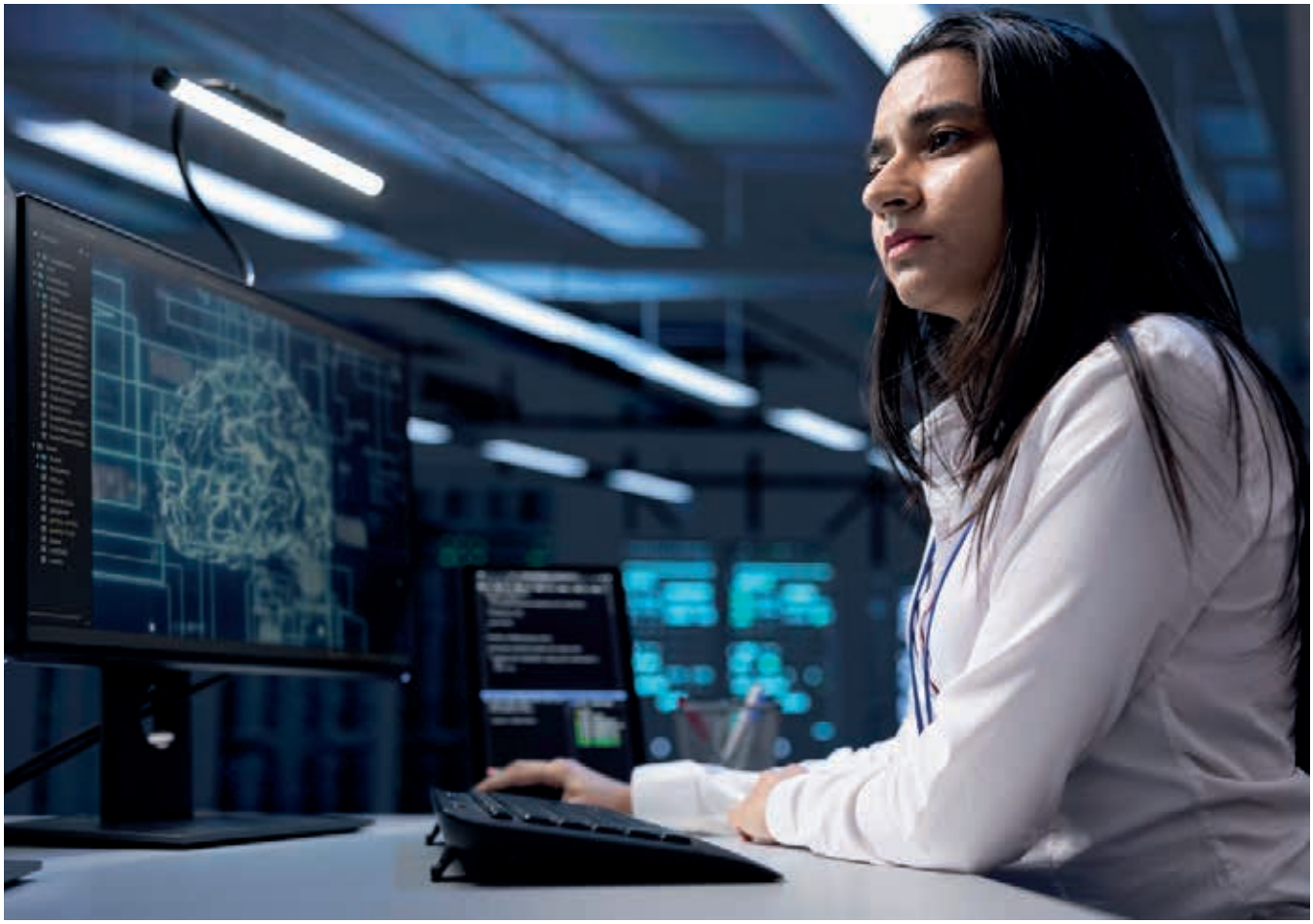
As digital transformation accelerates, NHI security is not optional, it's foundational. It's time to:

- recognise NHIs as first-class identities
- secure them with dynamic, least-privilege controls
- monitor them as rigorously as human users.

In cyber security, clarity is power, and you can't protect what you can't identify. ●

Abbas Kudrati is the Regional Chief Identity and Security Advisor at Silverfort, and a former Chief Cybersecurity Advisor at Microsoft Asia. With deep expertise in identity security, Zero Trust architecture, cloud and cyber security, he provides strategic and technical guidance to a number of startups – including SquareX, Aona.ai and PriviEzi – as well as leading institutions, such as EC-Council and St Vincent de Paul Society Victoria, while actively mentoring the cyber security community. A bestselling author and renowned keynote speaker, Kudrati has authored industry-leading books such as *Threat Hunting in the Cloud* and *Zero Trust Journey Across the Digital Estate*. He also serves as a Professor of Practice at La Trobe University and is a Fellow of the Australian Information Security Association.

Deakin ready to capture Australia's AI moment



AUSTRALIA'S ARTIFICIAL INTELLIGENCE (AI) landscape is rapidly evolving, with significant strides in adoption, research and governance. While AI presents exciting opportunities for national prosperity, it also raises ethical, security and trust challenges. As a national leader in applied AI and cyber security, Deakin University is addressing these challenges from Australia's AI hub, ensuring technological progress is responsible and resilient.

With expertise spanning AI, intelligent systems and cyber security, Deakin develops solutions that tackle national priorities across health care, defence, advanced manufacturing, and education. Through the Deakin Applied Artificial Intelligence Initiative, the Deakin Institute for Intelligent Systems, and the Deakin Cyber Research and Innovation Centre (Deakin Cyber), Deakin translates research into real-world impact, strengthening national resilience while driving economic and societal benefits.

A GROWING AI ECOSYSTEM IN AUSTRALIA

Australia's AI ecosystem is growing rapidly. According to the National Artificial Intelligence Centre, there are now more than 1500 AI companies across the country, including startups, scale-ups and established enterprises. AI research activity is booming, too: AI-related patents grew from 170 in 2015 to 629 in 2024, while AI publications surged from 5.3 per cent of total scholarly output in 2015 to 11.6 per cent in 2024.

AI is no longer confined to tech companies – its integration spans health care, defence, education, advanced manufacturing, agriculture and environmental science, driving efficiency and innovation across diverse sectors.

Workforce demand reflects this momentum. In 2024, more than 1500 organisations sought AI-related skills – a threefold increase since 2015.

DEAKIN'S LEADERSHIP IN AI AND CYBER

Deakin is shaping the future of AI through an ecosystem that connects research, industry collaboration, and workforce development. This leadership in AI and cyber security is powered by Deakin's world-leading research hubs:

1. Deakin Applied AI Initiative

The Applied AI Initiative is Deakin's flagship AI program, leading research in machine learning, computer vision, natural language processing and decision support systems. Its mission is clear: turn research into real-world solutions.

Through partnerships with government, industry and community organisations, the Initiative delivers projects that

not only advance technology, but also create measurable societal and economic benefits. From healthcare diagnostics to smart manufacturing and education technologies, the institute ensures innovation is practical, ethical and secure.

2. Deakin Institute for Intelligent Systems

Deakin's Institute for Intelligent Systems advances research into intelligent systems, robotics, autonomous platforms and simulation environments. Its applied research strengthens national capabilities in defence, transport and Industry 4.0, with expertise in human-machine teaming and agentic AI for decision-making. These advancements position Deakin as a critical partner in building Australia's resilience and security.

The institute has spearheaded life-changing projects. HERCULES (Haptically-Enabled Robotically Controlled Ultrasound Examination System) is a world-first remote ultrasound robot tested inside a hospital with real patients. This breakthrough technology has the potential to transform health care by delivering diagnostic services to regional and remote communities where access is often dangerously limited.

3. Deakin Cyber

Cyber security and AI are now inseparable. As AI systems become more pervasive, the risks of misuse, data breaches and cyber attacks continue to rise. Deakin Cyber addresses these challenges by developing real-world solutions for critical infrastructure protection, identity security and threat intelligence – both by harnessing the power of AI and by securing AI systems against adversarial compromise.

Deakin takes an integrated approach, combining applied AI, cyber security and education to ensure that innovation is advanced responsibly, securely, and with impact.

One example is the Augmenting Cyber Defence Capability project, a collaboration between Deakin Cyber, CSIRO's Data61 and Edith Cowan University through the Cyber Security Cooperative Research Centre. The project leveraged AI technologies including large language models (LLMs) to develop CyberAlly – an LLM-driven, knowledge graph-enhanced AI assistant that enhances the efficiency and effectiveness of blue teams during incident response.

These initiatives are strengthened by significant industry engagement and investment. Since 2019, Deakin Cyber has doubled its research income, reflecting the practical value and relevance of its work. Its partnerships with government, industry and community stakeholders demonstrate that trust, security and impact remain central to the responsible adoption of AI.

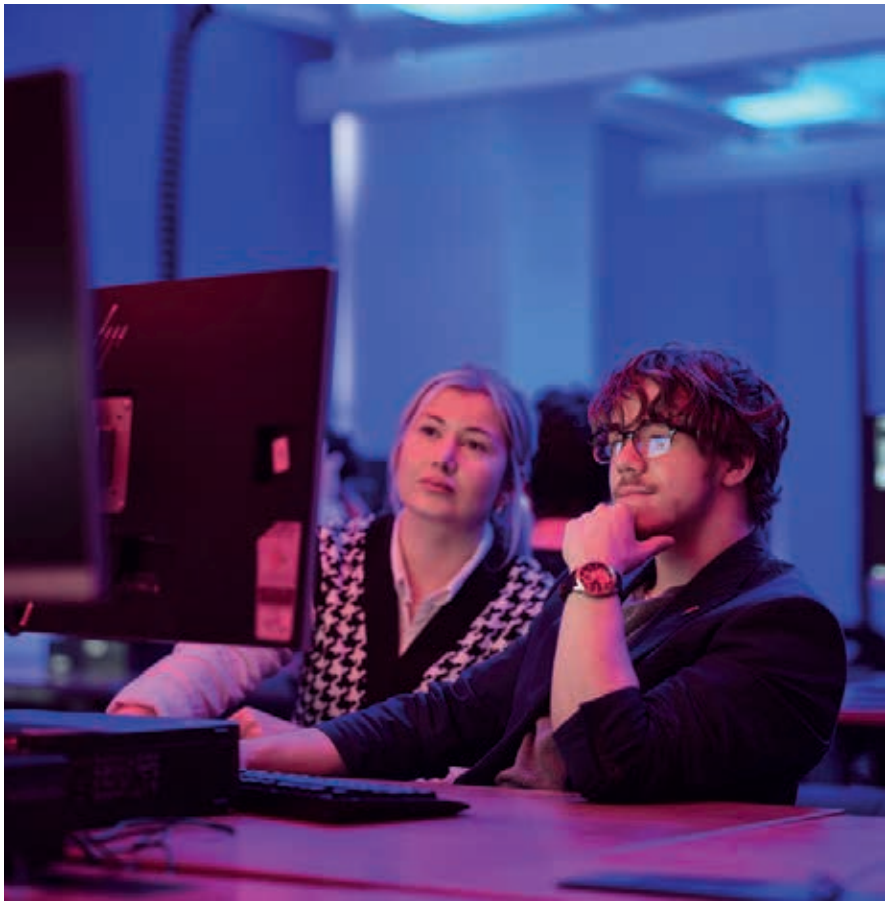
4. Deakin's Human-centric Technologies Research Group

The Human-centric Technologies Research Group is dedicated to fostering collaboration between humans and cutting-edge technologies. By integrating science, engineering, design and art with advanced technologies like AI, virtual reality, augmented reality and extended reality, the group creates innovative, AI-driven solutions to elevate cognitive and physical performance, and support people's wellbeing.

The group's Personalised AI + VR for Wellbeing in Isolation project addresses wellbeing in isolation, with applications in both health care and space. Designed to shift a user's emotional state from negative to positive via personalised, culturally appropriate immersive content, the project stands apart from conventional wellbeing interventions.

The group is also focused on researching how humans and AI can work together more effectively. Funded by the Asian Office of Aerospace Research and Development, the Ethical and Trusted Agentic AI for Human-Machine Teaming project is working on creating AI agents that act as trusted teammates in fast-moving, high-stakes environments.

The research is also focused on ensuring that these AI agents not only make smart decisions and collaborate with their human partners, but also behave ethically, follow rules, and align with human values. ●



When cyber reality hits home

BY DINESH DINO, WURTH AUSTRALIA

There is one cyber metric that every Australian board should be demanding.

It has been a bruising year for cyber resilience in Australia. In March, UniSuper, one of the country's largest superannuation funds, experienced a catastrophic outage due to a Google Cloud configuration mistake. This resulted in access being lost for more than half a million members for an extended period. In July, Qantas's Frequent Flyer database was exposed through a scraping breach that alarmed the aviation industry and prompted a swift response from the national airline. Additionally, an elite Australian university acknowledged that a sophisticated foreign actor had persistently targeted it. Researchers are concerned about the possible exfiltration of high-value intellectual property.

These events were more than just technical failures; they constituted strategic and operational crises. Services went offline, and customers lost trust. Institutional leaders faced public scrutiny. The most telling outcome, however, was the dramatic change in boardroom discussions. The focus shifted from how the breach happened to how long it took to recover, and what was done to prevent future failures.

Welcome to the new cyber normal. Prevention alone is no longer sufficient. Resilience now defines survival. In this evolving landscape, boards no longer focus solely on technical metrics like intrusion attempts or antivirus coverage. Instead, they are asking, 'If a cyber attack occurs today, how quickly can we fully recover?'

BEYOND THE DASHBOARD METRICS

Enter a typical boardroom for a cyber risk briefing and you will find an alphabet soup of metrics: mean time to detect (MTTD), mean time to respond (MTTR), phishing click-through rates, endpoint patching levels, CVE backlog, and maybe a NIST maturity model score. Each metric has technical utility, but few of them deliver business clarity. The reality is that traditional cyber security metrics speak to internal operations. They reflect activity, not outcomes. They are rarely aligned with what boards and regulators prioritise, which is the continuity of critical services, protection of customer trust, and assurance of rapid restoration.

Cyber security may be a technical function, but it is now evaluated by how well an organisation can sustain operations, protect value and regain normalcy after a crisis. This is why one metric is gaining serious traction among executive and risk leaders. It offers a clear answer to the most crucial question of all.

Dinesh Dino

CYBER RECOVERY TIME: THE METRIC THAT MATTERS MOST

Cyber recovery time (CRT) is the average time it takes for an organisation to fully restore its critical business operations after a cyber incident. CRT shifts the conversation from attack vectors and patch management to outcomes that matter to customers, shareholders, and regulators. Think of CRT as the equivalent of patient recovery time after major surgery. The condition may vary, but the goal remains the same: to return to full function as quickly and with as minimal impact as possible. CRT defines that goal in concrete terms. It focuses on how soon the enterprise can be fully operational again, regardless of the source of the disruption.

CRT offers three strategic advantages:

1. It is a business-first strategy. It frames cyber risk in terms of downtime, revenue loss and brand erosion – terms that executives and investors understand intuitively.
2. It is holistic. CRT covers the full spectrum of resilience, including detection, containment, coordination and restoration.
3. It is regulator-aligned. CRT resonates with emerging compliance regimes in Australia and abroad that emphasise operational resilience and timely recovery over traditional perimeter defence.

Let us explore why this metric is not only relevant, but also essential in the Australian context.

REGULATORY GRAVITY: CPS 234, SOCI, AND GLOBAL HARMONISATION

Australia's cyber security regulatory landscape has entered a new era. Where once it focused on information security frameworks and compliance checklists,

attention has now shifted to operational readiness and recoverability. The Australian Prudential Regulation Authority's (APRA's) CPS 234 regulation requires all APRA-regulated entities to maintain an information security capability commensurate with the threats they face. The implications are clear: if a business cannot restore its services quickly after an incident, it risks breaching its fiduciary duties and supervisory requirements.

The federal *Security of Critical Infrastructure Act 2018* (SOCI) also continues to expand its scope. Now covering sectors including higher education, energy, financial services, logistics, telecommunications and defence, it places a legal obligation on operators of critical infrastructure to demonstrate effective incident response and recovery planning.

On the global stage, CRT also closely aligns with the principles of the European Union's Digital Operational Resilience Act, and the United States Securities and Exchange Commission's new cyber security rules, both of which emphasise recovery planning and the disclosure of material impacts. For Australian organisations, this alignment means that CRT is not just a strategic choice, but is also a regulatory requirement. Boards will increasingly be judged not by whether they can prevent all attacks, but instead by whether they can recover from one before it causes systemic harm.

MEASURING CRT WITH DISCIPLINE AND PRECISION

A meaningful CRT measure requires more than intuition. It must be designed with specificity, rigour and relevance.

First, CRT must be accurate and clearly timed. It should be specified in hours or days, not vague estimates. If your CRT for core banking platforms is 24 hours, this informs both your customers and regulators about your downtime window.

Second, CRT must be scenario-based. A single number cannot capture the full range of threat types. The recovery time from a ransomware attack will differ significantly from that of a distributed denial-of-service attack or a software supply chain compromise. Measure CRT by the incident archetype to better reflect reality.

Third, CRT must align with business function tiers. Not all systems have the same level of impact. For instance, a Tier 1 system, such as a digital payments infrastructure, might require a CRT of 12 hours. Conversely, a Tier 3 HR application can tolerate up to three days of downtime.

Fourth, CRT must be tested through exercises. Conducting red team simulations, tabletop drills and controlled failover tests validates assumptions. These exercises uncover not only technical weaknesses, but also delays caused by human error, decision-making delays and failures by third parties.

Fifth, CRT must be benchmarked. Whether against industry peers, historical baselines, or internal risk tolerance levels, CRT gains credibility when contextualised. If your competitors average a 72-hour recovery window for ransomware, and your organisation still has a 120-hour recovery window, you have a clear performance gap. If you are trending downward year-over-year, it shows resilience maturity.

CRT IN THE BOARDROOM: ONE SLIDE, ONE TRUTH

One of the reasons that CRT is gaining traction at the board level is its communicability. Unlike sprawling cyber dashboards, CRT can be conveyed in one sentence: 'If we are attacked today, we will be back online in (X) hours.'

This clarity is what board members are asking for. It enables discussion around financial impact, risk appetite, customer trust and investment trade-offs. CRT transforms cyber security into a core business continuity issue. Board reporting should present:

- a top-line CRT value for each critical system tier
- the underlying data source, whether simulation, live incident or disaster recovery test
- a trendline of CRT over time, showing improvement or areas of concern
- an investment road map to reduce CRT to target levels.

This approach promotes proactive dialogue, rather than reactive explanations. It also instils confidence among stakeholders and regulators that the organisation isn't just focused on preventing incidents, but is also prepared to recover decisively from them.

WHAT HAPPENS WHEN CRT IS IGNORED?

Let's revisit the UniSuper incident. The cause, a misconfigured Google Cloud tenancy, was not malicious; however, the impact was indistinguishable from a cyber attack. Members were locked out of their accounts, and retirement savings could neither be viewed nor managed. The outage lasted for days, and the reputational damage was immense. The public and media focused not on the root cause, but on the recovery time. CRT, even if not officially reported, was the unseen metric by which UniSuper was judged.

Contrast that with Maersk's recovery from the NotPetya attack in 2017. Within 10 days, Maersk had restored full global shipping operations, despite losing 49,000 endpoints and 4000 servers. That rapid restoration was not luck; it was the result of a culture built around recovery, including a critical domain controller backup stored offline in Ghana. CRT became Maersk's best defence and its strongest reputational asset.

Australian businesses should take note. CRT may be the difference between a bad news cycle and a class action lawsuit. It may determine whether your customers wait patiently or flee permanently, and it will increasingly be what regulators measure when assessing your risk exposure.

FROM METRIC TO MANDATE: EMBEDDING CRT INTO STRATEGY

CRT is not just a risk dashboard item – it must become a strategic objective, embedded in business planning and enterprise architecture.

Achieving this requires the involvement of:

- technology teams, who must design systems with failover, backup and automation in mind
- security leaders, who must prioritise detection, containment and playbook orchestration
- business continuity planners, who must map recovery dependencies and rehearse responses
- executives and boards, who must allocate investment and define acceptable CRT thresholds.

It also demands a shift in thinking – from preventing every threat, to preparing for unavoidable disruption, monitoring firewall alerts, safeguarding operational continuity, and from isolated technical actions to unified enterprise resilience. When CRT becomes a shared performance metric across departments, it aligns everyone towards the same goal: recovery.

THE FINAL WORD: CRT AS AUSTRALIA'S CYBER RESILIENCE COMPASS

We are no longer immune to the effects of global cyber instability. Our financial systems, critical infrastructure, universities and cloud providers have all experienced severe disruption. The lesson is simple: resilience matters more than ever. CRT is the single most powerful metric for quantifying and communicating resilience. It speaks the language of outcomes, integrates technical and strategic functions, and satisfies the demands of regulators, shareholders, and customers alike. In a time when cyber incidents are increasingly unavoidable, your resilience will determine your strength. CRT is more than just a metric; it serves as a guide for your organisation towards preparedness, capability and trust.

Start measuring it. Start reporting it. Most importantly, start improving it. That is what will separate the survivors from the rest. ●

Dinesh Dino is a seasoned technologist and business leader with more than 20 years of global experience in cyber security, artificial intelligence (AI) and IT service management. He is currently pursuing a PhD and holds master's degrees in IT and cyber security, seamlessly integrating academic insight with practical application. As a GRC Specialist at Wurth Australia, Dino leads cyber security initiatives, drives IT compliance, promotes user education, and cultivates strategic external partnerships. His work is grounded in aligning governance frameworks with innovation and resilience. Dino, a recognised thought leader in policy development and technology entrepreneurship, bridges the gap between emerging technologies and business outcomes. As a lecturer, startup mentor and advocate for democratising AI, he is deeply committed to fostering innovation and capability-building across industries.

Cybersecurity solutions for your digital enterprise

Protect your business from internal and external threats with ManageEngine's IT security solutions.

ManageEngine

Our solutions

Cloud security for enterprise IT | Endpoint security | Network security | Identity and access management | Data security | Security information and event management | Privileged access management

cybersecurity.manageengine.com

Find ManageEngine at booth 35

ManageEngine is a division of **Zoho Corp.**

Canberra – Australia's (cyber) Capital Territory

BY DR VICKI GARDINER, CHIEF OPERATING OFFICER, CANBERRA CYBER HUB

CANBERRA IS AUSTRALIA'S cyber capital. It's no surprise; the region's businesses protect the nation's most critical assets, researchers solve global challenges with fresh thinking, and Canberra's workforce is the most educated in Australia.

When it comes to cyber, Canberra has long punched above its weight. The region is home to more cyber-focused small and medium-sized enterprises, prime contractors, and government agencies than anywhere else in the country. Close proximity to the federal government – Australia's largest buyer of cyber services – ensures a steady pipeline of contracts and innovation opportunities.

Under these conditions, researchers and companies alike have both the stability and opportunity to grow.

Take Australian National University's (ANU's) spin-out, Quintessence Labs, who are delivering quantum-enabled key generation and other world-leading cyber solutions to two of the most competitive global markets – the United States and European Union. There's also PentenAmio, a Canberra-based cyber technology company that began in 2014 with just four employees, and has since grown to a team of more than 300, serving clients nationally and across the globe. And then there's Instaclustr. Founded in Canberra in 2013, it became a global leader in open-source data technology. Its success drew the attention of cloud giant NetApp, which acquired the company in a deal reportedly worth more than $500 million in 2022.

With the foundations for cyber success already in place, the Canberra Cyber Hub (the Hub) was established to connect the dots and amplify Canberra's competitive advantage through one unified ecosystem.

Our ecosystem brings together:

- highly experienced companies already embedded with end users across government, defence and enterprise
- new and innovative companies developing solutions that use emerging technologies, such as quantum, artificial intelligence and machine learning, to protect us from increasing cyberthreats
- leading researchers from world-class institutions – including ANU, the University of New South Wales, the University of Canberra and CSIRO – working in partnership to transition brilliant ideas into commercial products.

The Hub's Cyber Directory makes this capability searchable by service, size and sector, listing more than 100 local businesses.

The Hub, however, is more than a directory; it's your door into Canberra's cyber ecosystem. We introduce local innovators to investors, match researchers with commercial partners, and help businesses to scale to national and international markets.

If you're not a local, the Hub can help you set up here – whether you need a hand to navigate the landscape, make the right introductions or find the partners who will help you succeed.

Whether you're looking to partner with our ecosystem or become part of it, it's time to take your place in Australia's cyber capital. ●

CANBERRA CYBER HUB

The **Canberra Cyber Directory** places capability at your fingertips – connecting you to **100+ leading cyber businesses**.

Easily filter by:

Capabilities

From cloud security to threat intelligence, find specialists in the exact services you need.

Ownership

Discover Australian-owned, veteran-owned, female-founded or Indigenous enterprises.

Sectors

Match with providers experienced in Defence, finance, health, critical infrastructure, and more.

Search the Directory
canberracyberhub.com.au/cyber-businesses

Beyond the hype: a business-first approach to AI governance

BY YVONNE SEARS, FOUNDER AND CEO, ELEV8 RESILIENCE

Why Australian organisations must return to fundamentals before embracing artificial intelligence.

Australia's artificial intelligence (AI) adoption rate has reached 90 per cent among surveyed organisations, according to the Governance Institute of Australia; yet, a startling reality emerges: only 25 per cent have comprehensive governance frameworks in place, as revealed by AuditBoard's 2025 research. This isn't just a compliance gap – it's a strategic vulnerability that could derail the very innovation that these organisations seek to achieve.

The AI revolution is well underway, and Australian organisations are eager to get on board. Within the Australian Government sector alone, 56 entities now report AI adoption, more than double the 27 entities recorded in 2022–23, according to the Australian National Audit Office. Yet, this enthusiasm for adoption significantly outpaces the establishment of robust governance frameworks to guide AI's use.

This mismatch is more than just a statistic; it's a warning sign. Without proper strategies in place, embracing AI can introduce significant risks. Drawing from my experience helping organisations implement AI from a business-resilience perspective, I've seen what happens when enthusiasm outpaces preparation. Too often, companies rush to experiment with new AI tools, looking for quick wins or fun applications, and end up forcing solutions where there's no clear need. In doing so, they overlook the essentials of change management and, more importantly, sound risk management.

THE FUNDAMENTALS GAP

The fundamental challenge facing organisations isn't just technological adoption; it's a lack of strategic discipline. Too often, businesses leap into AI initiatives without first examining the essential drivers for change. Critical questions are left unanswered: Which processes truly require improvement? What are the underlying business needs? How can technology be harnessed to address those needs, rather than simply overlaying new tools on old problems?

This tendency towards 'tool first' thinking exposes a deeper gap: many organisations have not updated their risk frameworks to account for the unique challenges that AI introduces. While information security concerns may go unaddressed, AI-specific risks (such as algorithmic bias, opaque decision-making processes and data quality issues) are frequently overlooked altogether. Employee training in AI tools is sometimes prioritised, but often lacks alignment with clearly defined strategic objectives. Without a foundational understanding of desired outcomes, organisations risk both ineffective implementations and missed opportunities for meaningful transformation.

This is where established frameworks like ISO 42001 become invaluable. The standard provides a structured methodology that requires organisations to clearly define their AI objectives before implementation, exactly the disciplined approach that's currently missing from many AI initiatives.


Yvonne Sears

Ultimately, the absence of rigorous, business-first analysis sets organisations up for avoidable pitfalls. Until these basics are addressed, the promise of AI will remain out of reach, and the technology's risks will continue to outpace its rewards.

A BUSINESS-RESILIENCE APPROACH TO AI GOVERNANCE

To build strong AI governance, organisations should apply the same disciplined methodology used for business-resilience planning. This starts with a deep understanding of what makes the business unique – its core purpose, essential operations and strategic objectives. Only then can leaders map out how these are supported by key processes, people, technologies and data.

With this foundation, organisations can accurately identify and assess their risk profile, including operational risks and areas ripe for improvement. The focus shifts from adapting the business to fit new technologies, to leveraging technology in a way that genuinely supports business priorities and safeguards continuity.

When guiding organisations back to these basics, I ask the difficult questions: What are the essential business objectives? How will AI support or threaten these goals? What specific operational and data risks are introduced?

By grounding AI governance in a business-resilience framework, organisations are better positioned to innovate confidently, withstand disruptions and ensure that the integration of AI delivers true value while protecting what matters most.

THE ISO 42001 FRAMEWORK: AUSTRALIA'S PATH FORWARD

ISO 42001, the world's first international standard for AI management systems, provides exactly the structured approach that Australian organisations need.

Unlike ad hoc governance attempts, ISO 42001 offers a comprehensive framework that addresses the full AI life cycle – from planning and development, to deployment and monitoring.

The standard's business-first approach aligns perfectly – it requires organisations to clearly define their AI objectives, assess risks systematically and implement controls that support rather than hinder innovation. For Australian organisations already familiar with ISO 27001 for information security, ISO 42001 provides a natural evolution that integrates AI governance with existing risk management practices.

What makes ISO 42001 particularly valuable is its emphasis on continual improvement and stakeholder engagement. The framework recognises that AI governance isn't a one-time implementation, but rather an ongoing process that must evolve with both technological advancement and business needs. This aligns with the business-resilience principles – building adaptive capacity rather than rigid compliance structures.

By systematically linking business processes (as we do in a BIA) and examining how AI supports these operations, organisations can better understand the criticality of each AI solution

THE AI IMPACT ASSESSMENT EVOLUTION

In today's rapidly evolving digital environment, the importance of robust AI Impact Assessments (AIIAs) cannot be overstated. Just as organisations routinely conduct business impact assessments (BIAs) and privacy impact assessments (PIAs), there is now a critical need to build similar rigour into how we evaluate the deployment of AI.

AIIAs serve as a strategic bridge between business objectives and technological innovation. By systematically linking business processes (as we do in a BIA) and examining how AI supports these operations, organisations can better understand the criticality of each AI solution. This includes considering the potential impact of losing access to an AI system or, perhaps more significantly, the repercussions of diminished trust in its outputs.

The methodology aligns closely with ISO 42001's risk assessment requirements, which mandate systematic evaluation of AI-related risks throughout the system life cycle. This integration ensures that AIIAs aren't standalone exercises, but are part of a comprehensive governance framework. Conducting an AIIA allows organisations to evaluate operational risks in tandem with anticipated returns on investment. The process not only highlights the issues at stake, but also reframes them – helping leaders to see challenges from a fresh, business-first perspective.

Since the assessment methodology aligns closely with established frameworks like BIA, PIA and ISO 27001, many organisations will find themselves on familiar ground when considering the impact on confidentiality, integrity and availability.

A key area often overlooked, however, is data quality. Without a clear understanding of what data is being used, why it's being used, and how it's governed, even the most promising AI initiatives are at risk of failure. Robust AIIAs demand that organisations establish and maintain strong data governance practices, ensuring that every AI solution is built on a foundation of accurate, reliable information.

In summary, integrating thorough AIIAs into organisational workflows is essential to unlocking AI's full value, managing risks and building lasting trust in intelligent systems. Only through this disciplined approach can organisations drive innovation with confidence and resilience.

THE DATA QUALITY REALITY CHECK

The core argument here is simple but crucial: organisations must resist the urge to rush headlong into AI adoption. Instead, progress should be intentional – built by design, not by accident. Deliberate planning and careful consideration form the backbone of resilient, trustworthy AI systems.

The imperative of quality data

A recurring reality in AI implementation is that investing time up-front to ensure data quality pays off exponentially in the long run. When organisations rely on incomplete, inaccurate or outdated data (or so-called 'dirty' data), the risks to outcomes and trust are profound. Retrospective fixes are often far more costly and disruptive than proactive governance.

Ensuring data quality means asking foundational questions: What data are we using, and why? Who verifies its accuracy and relevance? How do we safeguard data throughout its life cycle – from collection, through processing and use, to eventual disposal? Each step requires clear protocols and accountability.

Embedding data quality in risk frameworks

Most risk frameworks already encompass general threats, but AI introduces new dimensions. Bias, data lineage and automated decision-making require targeted evaluation. AIIAs should borrow from privacy and business-impact methodologies, specifically considering:

- What data feeds into the system, and what is its provenance?
- Is the data fit for its intended use, and does it comply with legal and ethical standards?
- How are confidentiality, integrity and availability maintained?
- What are the consequences of data errors or quality lapses on business outcomes?
- What validation, checkpointing and review mechanisms are in place before deployment?

ISO 42001 provides specific guidance on data management for AI systems, requiring organisations to establish and maintain processes for data collection, processing, and quality assurance. This systematic

approach ensures that data governance isn't an afterthought, but is a foundational element of AI implementation.

A commitment to quality data underpins trustworthy AI. By slowing down and prioritising robust data governance, organisations are better equipped to design intelligent systems that serve their strategic goals, manage risks, and build enduring confidence among stakeholders.

THE IMPORTANCE OF DEFINING RISK APPETITE IN AI DEVELOPMENT

Defining risk appetite is a critical step in the development and deployment of AI solutions. It serves as a compass that ensures innovation does not outpace the organisation's capacity to manage potential harms or unintended consequences.

Strategic alignment and clarity

Clearly articulating risk appetite anchors AI initiatives in the broader strategic direction of the organisation. It prompts leadership to consider: Which risks are acceptable in pursuit of innovation, and which are not? This clarity avoids misalignment between new technologies and core organisational values or business goals.

ISO 42001 emphasises the importance of defining risk criteria and risk appetite as part of the AI management system. This ensures that risk appetite isn't just a theoretical concept, but is also an operational tool that guides decision-making throughout the AI life cycle.

Guiding informed decision-making

A well-defined risk appetite empowers decision-makers at every stage of the AI project life cycle. It helps teams to distinguish between calculated risks that drive value and unacceptable exposures that threaten trust or compliance. This leads to more consistent, transparent and defensible choices regarding tool selection, data use, automation levels, and response strategies.

Embedding governance and trust

Integrating risk appetite into governance frameworks ensures that AI projects are subject to appropriate oversight. It facilitates checkpoints and review processes tailored to the level of risk that the organisation is prepared to accept. This not only strengthens accountability, but also builds internal and external trust as stakeholders can see that AI solutions are being managed responsibly.

Supporting adaptability and growth

An explicit risk appetite enables organisations to innovate with confidence. It provides the boundaries within which teams can experiment, adapt and respond to emerging opportunities or challenges in AI. As the strategic environment evolves, updating risk appetite ensures ongoing alignment with organisational objectives and market realities. For instance:

- risk appetite shapes the boundaries of acceptable AI innovation
- alignment with strategy ensures that AI supports (not undermines) core goals and values
- clear articulation fosters trust, accountability, and effective governance throughout development and deployment.

In essence, defining and updating risk appetite is not just a compliance exercise; it is a cornerstone of strategic, responsible and successful AI adoption.

FINAL THOUGHTS: ACTIONABLE INSIGHTS AND NEXT STEPS

The statistics are clear: Australian organisations are embracing AI at an unprecedented rate, yet governance frameworks lag dangerously behind. This gap represents both a significant risk and a competitive opportunity.

Those organisations that act now to establish robust AI governance will not only mitigate risks, but also position themselves as leaders in responsible innovation. Responsible AI adoption is not just about compliance; it is a strategic imperative that builds lasting value, trust and resilience.

By proactively defining risk appetite, embedding governance frameworks like ISO 42001 and fostering a culture of accountability, organisations can confidently harness AI's transformative potential while safeguarding what matters most.

The organisations that will thrive in Australia's AI-driven future are those that lead with strategic discipline, not just technological enthusiasm. The time for reactive approaches has passed – proactive AI governance is now a competitive necessity. With 90 per cent of organisations already adopting AI, but only 25 per cent having comprehensive governance in place, the opportunity for differentiation through disciplined implementation has never been greater.

The question isn't whether your organisation will adopt AI, it's whether you'll do so with the strategic rigour that ensures long-term success. ●

Yvonne Sears is the Founder and CEO of Elev8 Resilience, specialising in integrated business resilience strategies that combine cyber security, business continuity, privacy and AI governance. With qualifications including Master of Science Information Security, GAICD, CISM, and expertise in ISO 42001, she helps organisations across Australia build strategic approaches to emerging technology risks.

Become a leader in cyber security at RMIT University

Secure the future and lead the digital frontier.

IN AN ERA where cyberthreats are escalating in complexity and frequency, RMIT University's Master of Cyber Security program positions you at the forefront of digital defence. Designed for aspiring cyber security professionals, this program offers a comprehensive curriculum that blends technical expertise with strategic acumen, preparing graduates to protect and advance the digital infrastructures of tomorrow.

WHY CHOOSE RMIT'S MASTER OF CYBER SECURITY?

1. **Comprehensive curriculum:** RMIT's program provides a robust education that combines strong theoretical foundations with hands-on, practical experience. You'll delve into key areas, such as:
   - ethical hacking
   - digital forensics
   - cryptography
   - cyber security risk management
   - network security
   - software security
   - human factor security.
2. **Specialisation opportunities:** Tailor your learning through electives in threat analysis, cryptanalysis, security governance, risk management and compliance, or blockchain technologies
3. **Real-world experience:** Engage in realistic simulations and capstone projects that mirror the challenges faced by cyber security professionals. RMIT's strong industry connections allow you to work on projects that provide valuable, real-world experience, enhancing your job-readiness and employability.
4. **Industry engagement:** Benefit from RMIT's extensive network of industry partners. Through work-integrated learning experiences, you'll have the opportunity to apply what you learn in a professional setting, gaining insights and feedback from industry experts.
5. **State-of-the-art facilities:** Utilise cutting-edge cyber security software and simulated exercises to develop your skills. RMIT's facilities are designed to provide you with the tools and environment needed to excel in the field of cyber security.
6. **Global recognition:** RMIT University (ranked 123rd in the world by QS World University Rankings) is renowned for its high-quality education and research. Its Master of Cyber Security program is recognised globally, making you a competitive candidate in the international job market.

PROGRAM STRUCTURE

The Master of Cyber Security is a two-year full-time or four-year part-time program. The curriculum includes 10 core subjects, covering essential topics such as software security, encryption standards, authentication mechanisms, and risk and controls mechanisms. The program also offers elective courses, allowing you to tailor your education to your specific interests and career goals.

CAREER OPPORTUNITIES

Graduates of the Master of Cyber Security will be well-prepared for a variety of roles in the cyber security field, including:

- penetration tester
- cyber security risk analyst/consultant
- cyber security consultant
- network security engineer/consultant
- secure software engineer or DevSecOps consultant
- digital forensics analyst
- security auditor.

With the increasing importance of cyber security across all industries, your expertise will be in high demand, ensuring a rewarding and impactful career.

JOIN RMIT UNIVERSITY

Embark on a journey to become a leader in the fight against cyberthreats. With RMIT's Master of Cyber Security, you'll gain the skills and knowledge needed to protect critical digital assets and ensure the resilience of information infrastructures. Apply now and take the first step towards a secure and successful future. •

For more information, visit RMIT's program page and program structure.

RMIT UNIVERSITY

Ready for what's next

Explore Cyber Security at RMIT

CRICOS: 00122A | RTO: 3046

Less complexity, more confidence: true security starts with real clarity

BY PETER SOULSBY, DIRECTOR OF CYBER SECURITY, BRENNAN

'A BALL OF confusion, that's what the world is today,' so sang The Temptations, way back in 1970. Boy, if they could see the world now. The world of cyber security is not inoculated from complexity. For every challenge, there's a vendor promising faster, smarter, better. For every problem, a smorgasbord of cure-all tools – sales pitches full of fear, urgency and, of course, silver bullets.

Could that mean today's most valuable technology asset is clarity?

Partners that help businesses cut through the noise; that offer real-world, sequential and pragmatic advice on where to start, what matters, and how to move the needle; that might guide you to do two things that materially reduce your risk (rather than sell you 10 that leave you exposed) – these are the types of clarity that temper and harden security.

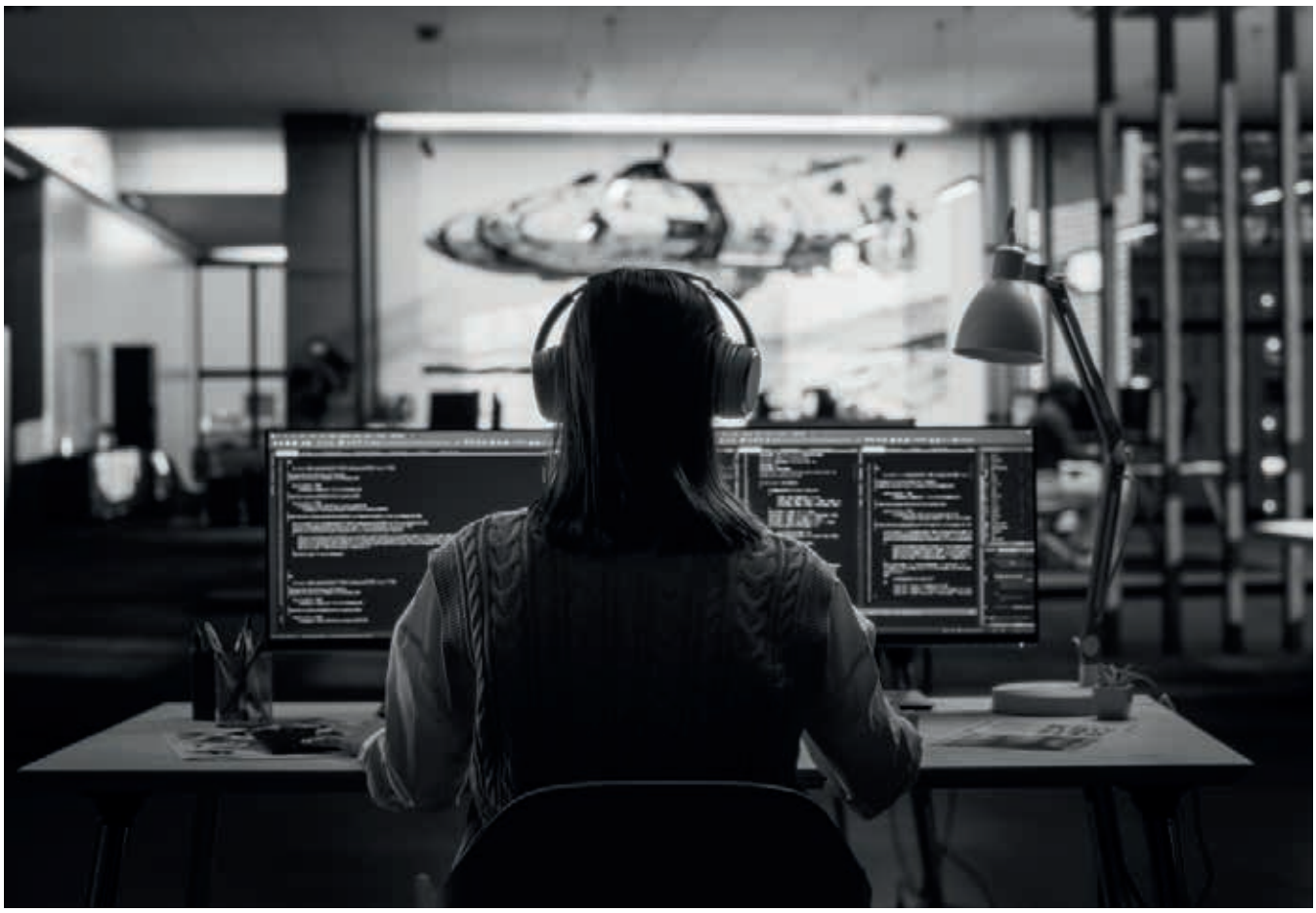
A good partner recognises that security isn't about how many products you've bought, or whether you tick every compliance box. Rather, it's about how effectively your defences align with your operational realities. When compliance adds unnecessary complexity, it begs users to find workarounds – and suddenly, your controls don't control anything.

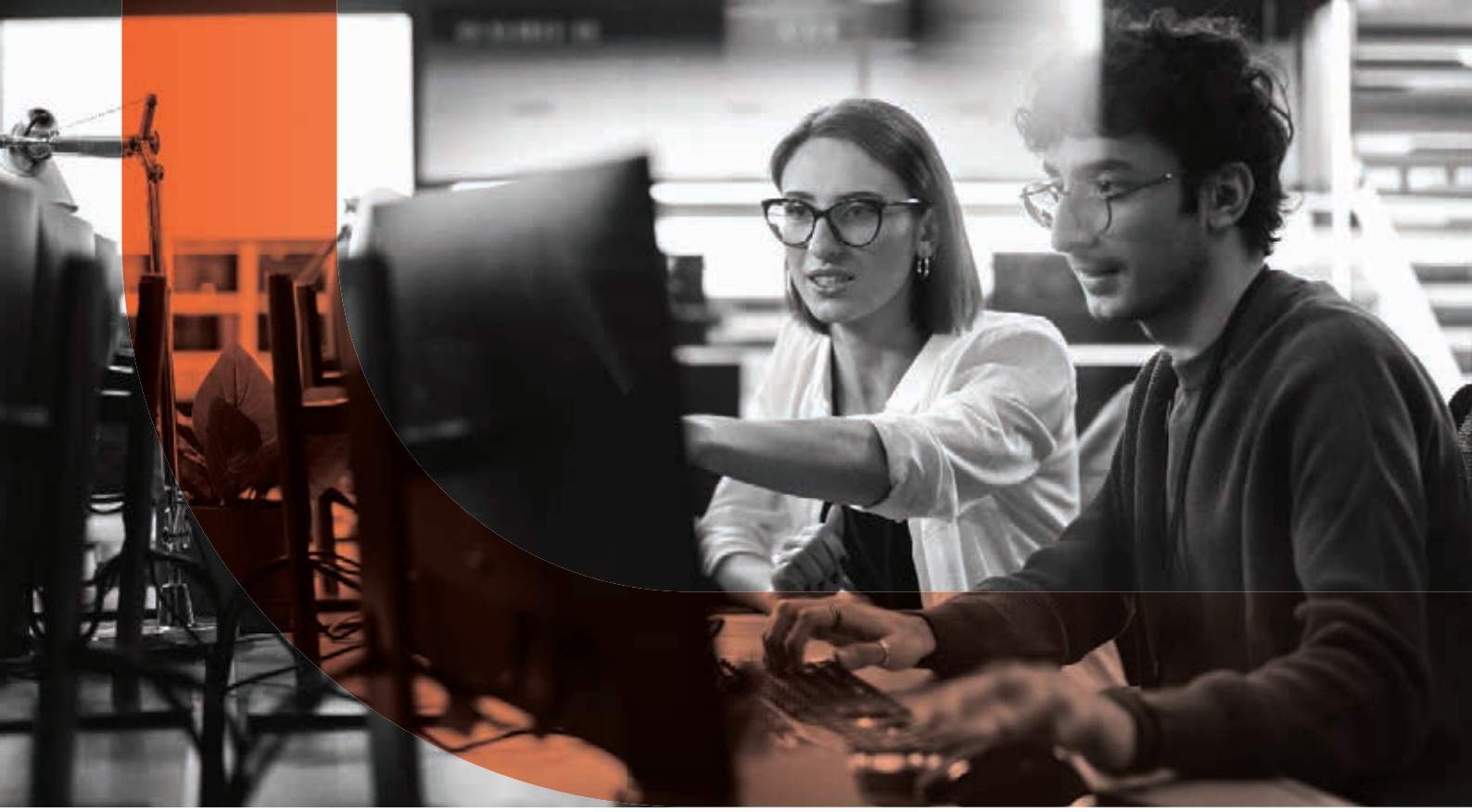
In a market full of noise and complexity, the best cyber security partners won't try to sell you the world; they'll help you do the right things, in the right order, for the right reasons – listening first, simplifying second, and only acting when it makes sense to your business, not theirs.

They also understand that automation has limits. Not everything can (or should) be handled by artificial intelligence. When you're entrusting the integrity of your systems and data, there's value in real experts providing real validation. A capable partner puts experienced people at the heart of their model, ensuring you can question assumptions, pressure-test outcomes, and trust the response.

The best cyber security providers take time to listen, to understand what's keeping you up at night, and to map a pragmatic, sequential approach that you can take to your board with confidence. They make the complex navigable, offering guidance instead of guesswork.

Cyber security isn't something you buy; it's the clarity you create – thoughtfully, incrementally, intelligently, and always with your business reality in mind. The world will always be confusing, but at least you'll know where you stand. •





300+ cyber experts. 24/7/365 proactive protection. True security starts here.

Experience multi-layered cybersecurity across every link in the chain.

Brennan's early years in emergency system recovery means we understand the true cost of system outages, failures and breaches better than anyone.

That's why we have developed a market-leading, systemised security culture that embeds protection into every aspect of your technology ecosystem, from advisory and architecture through to risk identification, response and rapid recovery.

With over 300 security experts, a 24/7/365 SOC, and a 'secure always' culture, we build multi-layered security standards into the core of everything we do to protect everything you do, blending global standards with sector-specific safeguards that reflect your actual risk profile.

And our True Performance System ensures we work closer, think sharper, and deliver measurable results to help you unlock new levels of security, stability, and reliability across networks, infrastructure, applications, control systems, and beyond. Because we're all about technology that works, not technology you're sold.

brennan_

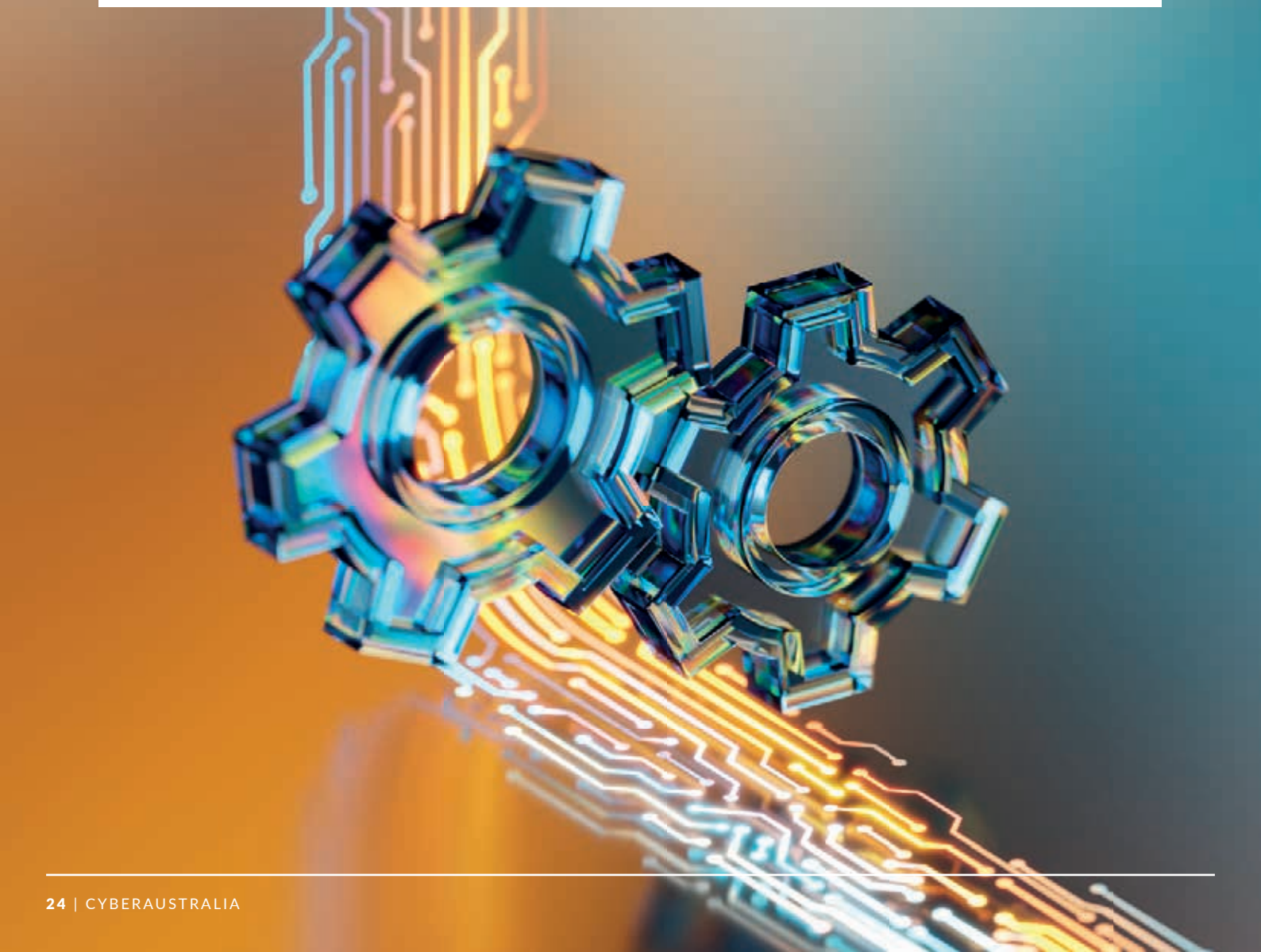
Let's connect.

brennanit.com.au
1300 500 000

Automation meets expressivity: a new step for formal methods in cyber security

BY PROFESSOR CEZARY KALISZYK, SCHOOL OF COMPUTING AND INFORMATION SYSTEMS, THE UNIVERSITY OF MELBOURNE

Watching the horizon for important evolutions in computing that will impact the world of cyber security turns up interesting advances in formal methods of verification.



In the security world, few tools are as powerful as formal methods. These methods are a set of mathematically rigorous techniques and tools that provide a kind of 'safety net'. Using these, it is possible to rule out entire classes of attacks, without onerous testing or simulation. These methods allow researchers to prove that a system satisfies key security properties. This field is particularly valuable in high-value settings, when a missed vulnerability can be catastrophic, such as in medicine and aviation.

At present, formal methods are divided into two main strands. On one side, there are interactive theorem-proving systems. They are often based on type theory that let researchers and developers describe subtle properties of data structures and software. With type theory, for example, we can express directly in the type system that a list has at least one element, which makes it impossible to try to get an element of an empty one.

On the other side of the spectrum are approaches that emphasise automation. These systems can handle large verification tasks automatically, sometimes at industrial scale, but they usually achieve this efficiency by working with less-expressive logics. They cannot capture all the subtle invariants of complex data structures, nor the full richness of modern software.

In practice, this means that automated tools can prove certain properties quickly, but they are forced to leave out the deeper guarantees that researchers and system designers often want in practice.

The Holy Grail has been finding a middle ground: a framework expressive enough to capture the rich invariants of complex software systems, while still amenable to efficient automated reasoning. Despite the great challenge of reaching this middle ground and the relatively slow pace of progress, researchers keep at it because of the immense value of such systems.

DEPENDENT HIGHER-ORDER LOGIC

Dependent higher-order logic (DHOL) extends higher-order logic with dependent types. These types mean that the type of something can depend on a value; thus, instead of saying 'This is a list of numbers', you could write 'This is a list of numbers that always has length 5.' DHOL means the compiler itself can enforce invariants that would otherwise require painstaking manual proofs. For example, in red–black trees – an essential data structure in many secure systems – the balancing invariants can be typed so that they are guaranteed by construction. In other words, if you try to write code that builds a broken tree, the compiler will reject it immediately. You cannot even write a red–black tree that violates its constraints; the type system rules it out before it ever runs.

Our research team has developed a native prover for DHOL that provides both soundness (it only proves true statements) and completeness (it can, in principle, prove any statement expressible in the logic). This combines strong expressivity of dependent types while opening the door to fully automated reasoning.


Professor Cezary Kaliszyk

Of course, like most frontier thinking research, there are caveats. Today, the completeness relies on relatively slow enumeration techniques. In practice, this means the prover can be too inefficient for large-scale security verification tasks – for now; however, this won't be forever. The next important step in our discipline's march forward will be optimising these procedures for performance. Once that happens, DHOL can become a practical tool for real-world systems and software.

TOWARDS SECURE SYSTEMS

Why does this matter for cyber security? Security failures often arise from overlooked edge cases or subtle invariant violations. Attackers exploit the fact that protocols or software components behave correctly under common conditions, but fail under rare ones. By encoding such invariants in dependent types, and proving them automatically in DHOL, we can close those gaps. Better still, we will be able to close those gaps quickly and without the expensive overhead of constant testing.

Currently, DHOL still has a way to travel before it can be deployed directly to verify real-world systems. The prover itself provides a strong foundation, but it can still be optimised for performance by integrating strong heuristics and learning for reasoning. The next step is to extend the reasoning already present in the logic while maintaining automation. These improvements will make DHOL more widely applicable and bring it closer to practical security verification.

LOOKING AHEAD

The development of DHOL shows that the traditional trade-off between automation and expressivity is not absolute. By combining dependent types with automated reasoning, it is possible to imagine tools that both capture the fine structure of data and protocols, and verify them automatically. While the system is not yet efficient enough for deployment, it marks a concrete step toward scaling formal verification to the complexity of real-world cyber systems. ●

Professor Cezary Kaliszyk is a Professor in the School of Computing and Information Systems at The University of Melbourne. His work spans automated reasoning, formal verification, and the intersection of logic and computer science. Through collaborations across Europe and Australia on DHOL and others, he is advancing the frontier of how mathematics and computation can safeguard digital society. To read more about his work, read his paper at: https://ckaliszyk.github.io/d/24/jncbck-ijcar24.pdf

Secure an income while securing your future in cyber security

EDITH COWAN UNIVERSITY (ECU) is creating opportunities for students to earn while they learn, providing a paid internship program with global technology giant IBM and its clients right across Western Australia.

The successful program focuses on high-demand skill areas key to Western Australia's digital economy, with ECU graduates working in the industry as software engineers, data scientists, mobile application developers and project managers – many of them straight out of university.

Jakub Antoniewicz is one of them, securing a full-time job as an applications engineer with IBM during his internship, while completing his final year of a computer science degree, majoring in software engineering.

'That was a great way for me to prepare for the workforce,' says Antoniewicz. 'During my internship with IBM, I got to develop an internal application for a client that I continued to work on during my graduate position, which is now used by over 300 unique users every week.

'It's extremely rewarding to be able to get an opportunity that allowed me to help people so quickly in my career.'

WORK-INTEGRATED LEARNING WORKS

According to ECU alumnus Dr Christopher Bolan, work-integrated learning (WIL) is a significant opportunity for all involved.

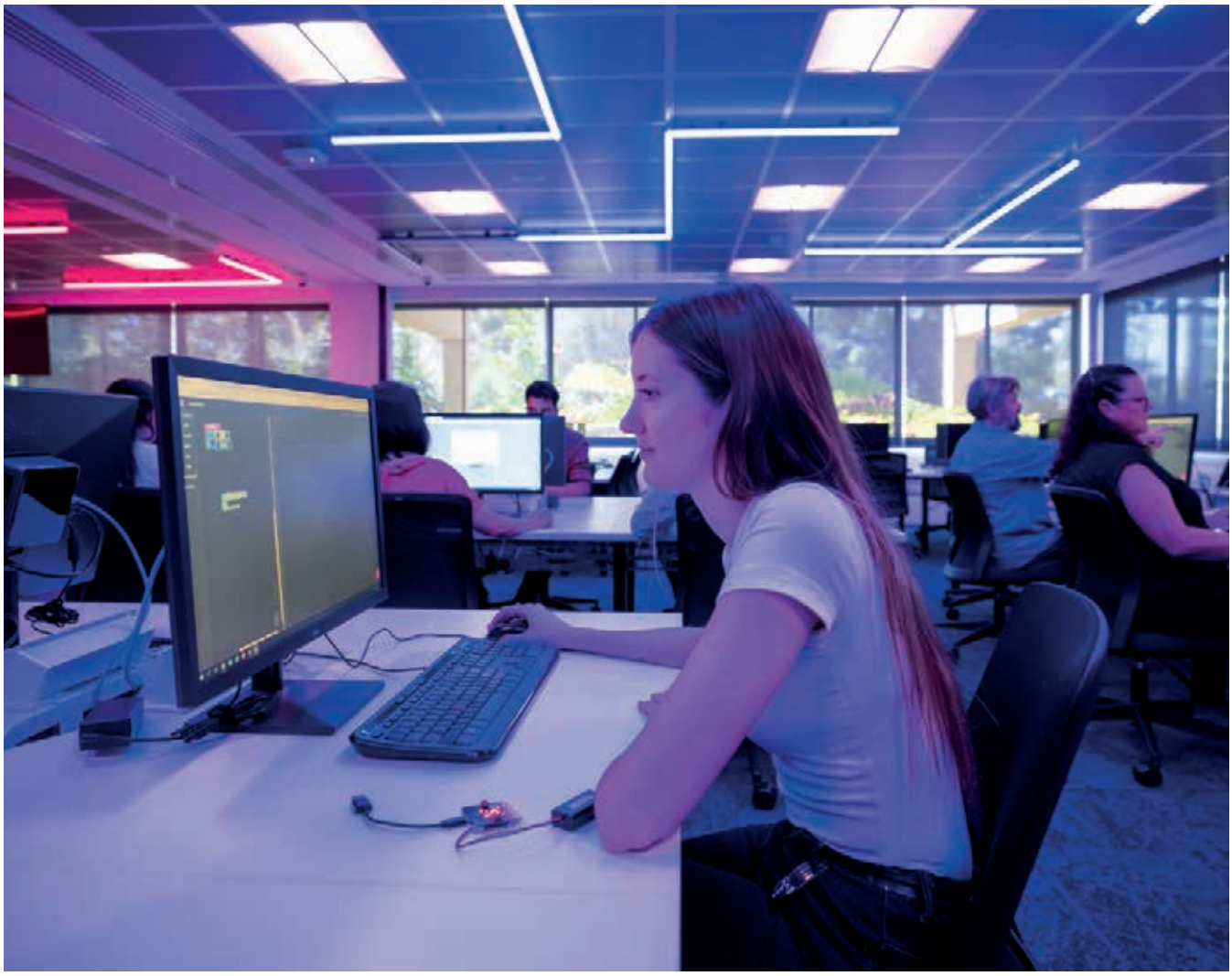
Co-founder of successful cyber company Seamless Intelligence, Bolan says his team fosters students' potential each year through the program.

'The ECU WIL program is fantastic for both students and the industry. It gives the students real-world experience within well-known companies in their chosen sector, and therefore increases their employability post graduation,' says Bolan.

'Our approach has been to create projects that explore new ideas. This gives the students a chance to extend their skills without some of the pressures or demands of customer-facing work.'

AUSTRALIA'S BIGGEST CYBER SECURITY CENTRE AT YOUR FINGERTIPS

ECU is home to one of Australia's largest security operations centres for teaching purposes – the first of



its kind in an Australian university, and one of only a handful worldwide.

It's in this world-class facility that cyber security experts investigate the nature of ransomware attacks and develop countermeasures. The facility gives students the opportunity to gain the real-world skills needed to thrive in any cyber career.

Speaking of unique facilities, from February 2026, postgraduate cybersecurity and computer science students will be among the first cohort to experience a university campus like no other.

The university's groundbreaking ECU City Campus opens its doors, revealing an incredible mix of technology, industry and creativity in Perth CBD. That includes a security operations training centre.

As ECU Vice-Chancellor Professor Clare Pollock says, 'We're not just building a university campus; we're creating a community and an environment for learning, for discovery, and for engagement. ECU City will be a special place for all Western Australians to connect with education, industry, creativity and the arts – right in the heart of Perth.'

STUDY OPPORTUNITIES AT ECU CITY

ECU's School of Science is offering postgraduate courses at the new campus for people wishing to progress their careers or who may be looking for a new career direction.

This includes a Graduate Certificate of Cyber Security, which is able to be completed in as little as six months full-time, and offering the flexibility of on-campus or online study.

A two-year full-time Master of Cyber Security degree is also offered, designed to address the needs of industry for cyber security professionals within government, law enforcement and industry.

A two-year full-time Master of Computer Science will enable people seeking to enter the IT profession with no previous experience in the computing discipline. The curriculum and capstone components of this course are heavily influenced by industry, offering students the opportunity to apply their expertise in real-world situations.

STUDY OVERSEAS WITH ECU'S UNIQUE DUAL DEGREE

Among the courses offered by ECU's School of Science for students considering studies in security and intelligence is a unique dual degree that involves one year of study at the University of Portsmouth in the United Kingdom.

The Bachelor of Science (Cybercrime, Security and Intelligence) requires students to spend the first two years of study at ECU, then live and study at the University of Portsmouth, before returning to ECU to complete the final six months of the course.

Cybercrime student Jacob Oskam from Perth spent a year studying in the United Kingdom as part of the dual-degree program, and says it's the best thing he's ever done.

Students like Oskam benefit from being educated by experts from two globally respected universities and gaining an understanding of different cultures that will help them to work more effectively with people from different backgrounds.

Ultimately, students graduate with two degrees, study for less time overall than they would for a double degree, and they get to see the world.

WORLD-CLASS TEACHING STAFF

ECU's Professor Paul Haskell-Dowland was recently inducted into the Australian Computer Society Hall of Fame. He has more than 25 years' experience in cyber security research and education in the United Kingdom and Australia, and is a global leader in the field.

This honour recognises Haskell-Dowland's outstanding contributions to the field of ICT in Australia, and underscores ECU's leadership in computing and cyber security education.

Haskell-Dowland is the Professor of Cyber Security Practice and Associate Dean for Computing and Security in the School of Science. He is also Australia's representative on several international committees, including the International Federation for Information Processing and Information Security Management. ●

To learn more about how to secure your cyber security future, visit ecu.edu.au/cyber-security

Security readiness starts with governance and people

BY JEREMY DALY, CYBER SECURITY LEAD, LUMIFY WORK

RECENT EVENTS AND reports continue to highlight a sobering reality: strong cyber security isn't just about technology, it's about leadership, culture and people.

In late July 2025, the Australian Prudential Regulation Authority (APRA) issued a formal reminder to superannuation fund board chairs, reinforcing their obligations under Prudential Standard CPS 234, which was a direct result of credential-stuffing incidents affecting several funds earlier in the year.

APRA's guidance instructed entities to review their current security controls and – where robust authentication such as multi-factor authentication is missing or inadequate, and where this was the case – notify APRA of any material control weaknesses within a determined timeframe and take corrective action.

This directive is more than a regulatory check box. It signals a shift: boards and executives are increasingly expected to play an active role in maintaining cyber security resilience. The days of leaving security solely to the IT department are over. Without executive leadership driving security governance, internal uplift efforts risk becoming directionless or ineffective.

This theme of inadequate governance is echoed in the New South Wales Auditor-General's Cyber Security Insights 2025 report. Despite having cyber security policies in place, many NSW Government agencies remain exposed.

The report found that 69 per cent of 'Protect' controls under the NSW Cyber Security Policy weren't fully implemented, and 152 high or extreme risks remained unresolved. Alarmingly, 59 per cent of agencies lacked independent assurance over their cyber self-assessments.

The private sector isn't immune, either. Many organisations fall into the same traps – relying on policies and frameworks without embedding cyber security into the fabric of business operations, failing to assign clear accountability, and neglecting to treat cyber risk as an enterprise-level concern.

The common denominator? A lack of governance, assurance and investment in people.

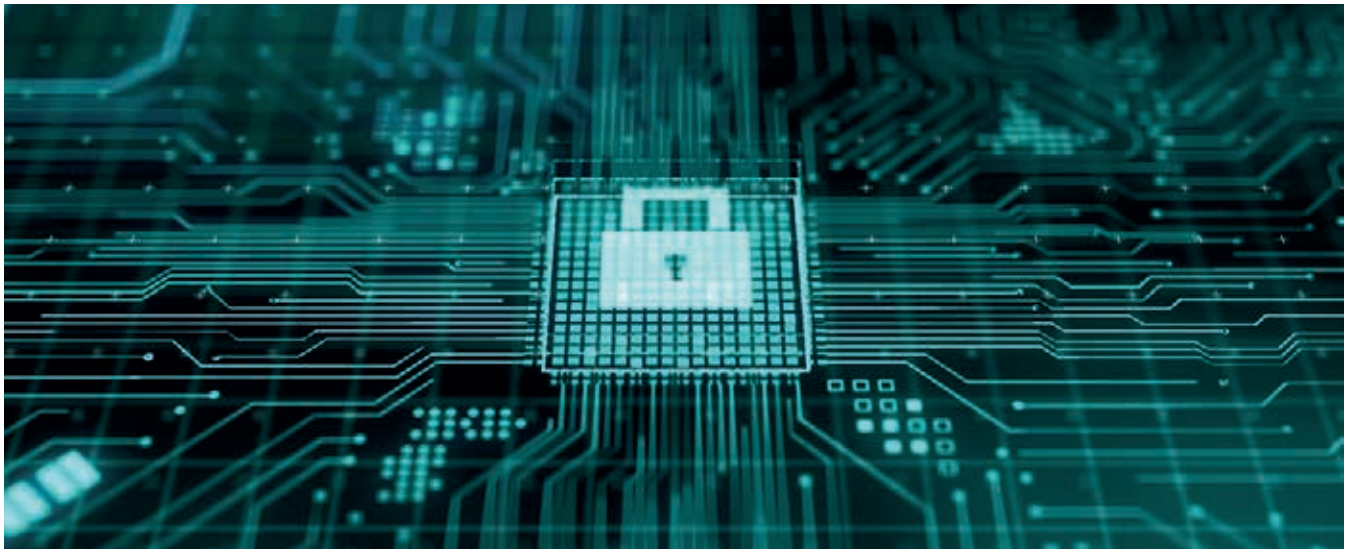
Security readiness is not built solely through tools and frameworks. It is sustained through a well-informed, accountable leadership team, a strong governance model, and a culture of cyber awareness across all levels of the organisation.

Jeremy Daly

Independent assurance is critical – not only to validate current controls, but also to provide stakeholders – such as our leadership, executives and boards – with the confidence that their strategies are being executed.

Ultimately, for organisations to maintain security readiness in an environment of increasing threats and regulatory scrutiny, we must focus on building resilient organisations from the top down. This means investing in our people – from directors to delivery teams – to ensure that they have the capability, authority and awareness to manage cyber risk effectively.

Cyber resilience isn't a destination. It's an ongoing journey, and leadership must lead the way. ●



LUMIFY work

Cyber Security Training Business of the Year

Explore authorised cyber training and certifications with Lumify Work (formerly DDLS Training).
Scan the QR code or visit:

https://link.lumifygroup.com/lumifyworkcybercon25

ISACA Accredited Elite Partner

ISC2 Official Training Preferred Partner

CompTIA Authorized Partner | Gold Partner

CertNexus Authorized Training Partner

Practical DevSecOps

PECB Authorized Gold Partner

OffSec | Channel Partner

EC-Council Accredited Training Center

AI security by design

BY RAKESH SHARMA, CHIEF ADVISOR, CYAIFI

Building trust and resilience across the artificial intelligence life cycle.

As artificial intelligence (AI) becomes more deeply integrated into our daily lives and business operations, traditional cyber security approaches are no longer enough. AI introduces new and complex risks that require us to rethink how we build and protect these systems. A key shift is adopting a 'Secure by Design' approach – where security is built into products from the very beginning, not added as an afterthought. By focusing on security throughout development, organisations can catch and prevent issues early, before products go live.

This is especially important for AI, which faces unique threats. Attacks like data poisoning, prompt injection and malicious model tampering can undermine the system even before it's deployed. And because AI can make autonomous decisions, a single compromise could cause real-world harm.

That's why security needs to go beyond just protecting code – it must also safeguard the data and ensure the model's behaviour is trustworthy. This requires a cross-functional approach involving developers, security experts, data scientists and leadership from the start.

FOUNDATIONAL PRINCIPLES FOR SECURE AI: ADAPTING CORE CYBER SECURITY FOR AI

A robust framework for safeguarding digital assets is provided by fundamental IT security principles, often referred to as 'core principles' or 'security fundamentals'. These principles guide organisations in building resilient systems, and include:

- **Confidentiality:** Ensuring that information is accessible only to those who have authorised access rights, protecting sensitive data from unauthorised disclosure.
- **Integrity:** Maintaining the accuracy and trustworthiness of data and systems, preventing unauthorised tampering or alteration.
- **Availability:** Guaranteeing that information and resources are accessible and usable when needed, minimising downtime.
- **Least privilege**: Granting users and processes only the minimum level of access and permissions necessary to perform their tasks, thereby limiting the potential impact of security breaches.
- **Defence in depth:** Employing multiple, overlapping layers of security controls and measures to protect systems and data, ensuring that if one layer is breached, additional layers provide protection.
- **Fail-safe defaults:** Basing access decisions on explicit permission rather than exclusion, meaning that the default should be to deny all access, and then explicitly permit only what is necessary. This approach is safer as mistakes tend to refuse permission, which is quickly detected.
- **Complete mediation:** Requiring that every access to every object must be checked for authority, every time, without relying on previous checks. This promotes a system-wide view of access control.
- **Open design:** Asserting that the design of a system should not be kept secret. Security mechanisms should depend on the secrecy of specific, easily protected keys or passwords, rather than on the ignorance of potential attackers.
- **Psychological acceptability:** Designing security systems for ease of use for humans, ensuring users routinely and automatically apply protection mechanisms correctly.

Core security principles like 'defence in depth' and 'open design' still apply to AI, but they need to be adjusted. For AI, protecting just the code isn't enough – you also need to secure the data, monitor the model's behaviour and be ready to respond if something goes wrong.

AI models, especially deep learning ones, are often hard to understand – even when the code is open. That's why we need explainability: giving clear insights into how and why an AI makes decisions. This helps make AI systems safer, more transparent and easier to trust, even when they're complex.

SECURING AI THROUGH ITS LIFE CYCLE: A PHASE-BY-PHASE APPROACH

To truly secure AI systems, we need to think about security at every stage of their development – not just at the end. Taking this proactive approach helps catch and fix issues early, instead of trying to patch them after the system is built. The process of developing AI usually goes through several phases, starting with defining the problem, and continuing all the way to ongoing monitoring and maintenance after deployment. Making security a part of each of these stages is key to building safe and trustworthy AI.

Phase one: problem definition and design (NIST AI-RMF: GOVERN and MAP)

The first stage of AI development is the most important for setting up strong security. Instead of treating security as something to add later, it should be built in from the very beginning and supported by leadership. That means clearly defining security requirements early, following principles like the United States Cybersecurity and Infrastructure Security Agency's 'taking ownership of customer security outcomes'.

It's also important to think ahead about how the system might be attacked. This involves creating a threat model that looks at every part of the AI pipeline – from how data is gathered and prepared, to how the model is trained and deployed. Early planning helps spot risks like data manipulation or system misuse before they become serious problems. Some of the key risks to watch out for include:

- data poisoning (inserting bad data into the training set)

- model inversion (extracting sensitive data from the model)
- model reconnaissance or supply chain attacks (exploiting pre-trained models, datasets or libraries).

Frameworks like MITRE ATLAS are helpful for identifying these types of threats. They highlight risks such as:

- machine learning supply chain compromise – vulnerabilities in the tools, data or models used
- model reconnaissance – attackers testing how the model reacts to inputs
- exfiltration via inference – pulling out private data just by using the model.

To deal with AI-specific risks, teams can use MLSecOps, which brings security practices from DevSecOps into machine learning. This means tracking where models come from, what data they use, and which tools are involved, making everything more transparent and trustworthy.

When MLSecOps and threat modelling are included early in development, security becomes more than just fixing bugs; it encourages teams to think about ethics, fairness and potential harm from the start. This leads to building AI systems that are not only secure, but also responsible and aligned with real-world values.

Example: Imagine a team is building a new AI-powered fraud-detection system. Right from the beginning, they make privacy a priority by choosing federated learning, which allows them to train the model without collecting all the sensitive financial data in one place. They also create a threat model to look for ways attackers might try to sneak bad data into the training process. On top of that, they plan adversarial testing to make sure that the model can't be easily tricked once it's live. By thinking about these risks early, the team builds strong security and ethical protections directly into the system's design.

Phase two: data collection and preparation (NIST AI-RMF: MEASURE)

This stage of AI development is where privacy risks can either creep in or be effectively managed. A key rule here is data minimisation, which means only collecting the information that's absolutely necessary. It also involves steps like anonymising data, reducing detail (like rounding timestamps to the nearest hour), and deleting data as soon as it's no longer needed.

To go further, teams can use advanced privacy-preserving techniques. For example:

- Differential privacy adds a bit of noise to the data so that individual records can't be traced back to real people.
- Federated learning trains AI models across multiple locations without needing to gather all the data in one place.
- Synthetic data is another option – it's artificially created, but still reflects real-world patterns, helping to protect privacy while enabling useful training.

Data integrity and bias also play a major role in keeping AI systems secure. If training data is biased or tampered with, it can lead to serious issues. For instance, attackers might try data poisoning – sneaking harmful inputs into the data so the AI learns the wrong things. This can result in models that are inaccurate, unfair or even dangerous.

To prevent this, teams should:

- run fairness audits to find hidden patterns (like ZIP codes or language) that might unfairly impact certain groups
- be careful with manual data labelling, since human annotators could see sensitive information. This can be managed by anonymising the data and limiting what annotators are allowed to see.

In short, poor data quality and unchecked bias aren't just performance issues; they're real security risks that attackers can exploit. Fixing them early helps to build safer, more trustworthy AI systems.

Example: A healthcare team is developing an AI system to help diagnose diseases. The team collects only what's necessary – like symptoms and lab results – and use differential privacy to hide personal identifiers. Before training the model, the team performs fairness audits to make sure the data doesn't over-represent certain groups, helping to prevent misdiagnosis in under-represented communities. This careful approach helps to protect both privacy and fairness from the start.

Phase three: model training and evaluation (NIST AI-RMF: MANAGE)

The model training phase is a critical point for making sure that AI systems are secure and reliable. Developers need to use secure coding practices designed for AI – like checking inputs and cleaning outputs – to prevent the model from acting unpredictably or making unsafe decisions.

It's also important to start with clear goals and test the model thoroughly. This includes adversarial testing (where the model is challenged with tricky inputs to see how it reacts) and red teaming (which simulates real attacks to find hidden weaknesses).

Another key part is securing the AI supply chain. That means checking all external libraries, datasets and pre-trained models for security issues before using them, since any of these could be a weak spot for attackers.

AI systems don't behave like regular software. Their risks often come from how data and the model interact, not just from code bugs. That's why behavioural and adversarial testing is so important – it helps catch problems that traditional testing would miss.

Example: While training an object-detection model for a self-driving car, the team uses adversarial training to help the system recognise stop signs – even if someone tries to fool it by adding stickers or distortions. They also carefully review every third-party library and pre-trained model they use, making sure there are no known security issues before adding them to the development pipeline.

Phase four: deployment and inference (NIST AI-RMF: MANAGE and GOVERN)

Once an AI model is deployed, it becomes exposed to new risks – especially adversarial inputs and application programming interface (API) misuse. If the APIs aren't properly secured, attackers could gain unauthorised access, so it's critical to use strong encryption for both data at rest and data in transit.

During deployment, key security principles matter more than ever:

- 'Least privilege' means that the AI system should only have the minimum access it needs – no more. If it doesn't need to read sensitive data or run certain commands, it shouldn't be allowed to.
- 'Complete mediation' ensures that every request, action or interaction with the AI – like accessing data or triggering a prediction – is checked for authorisation. Nothing should bypass these controls.
- 'Secure by default' means that if something fails, the system should fail closed – denying access rather than accidentally granting it.

One key aspect of AI security is explainability. If we don't understand how an AI system makes its decisions, it's harder to test, trust and protect. Tools that explain a model's behaviour after it has been deployed (post-hoc explainability) help us review its decisions, catch issues and respond quickly when something goes wrong.

AI systems that act on their own – like autonomous bots or agents – pose even more risk. If they're not closely managed, they could take actions that are unsafe or harmful. That's why behavioural monitoring is so important – it helps spot when the AI starts doing something unexpected.

Unlike regular software, AI models can change over time based on the data they receive or the environment they're in. So, even if a model is safe at launch, new risks can appear later. That's why AI security can't be a 'set and forget' approach. It needs real-time monitoring, regular updates and adaptive controls to keep up with changing threats.

Example: A financial firm deploys an AI-powered trading bot. To secure it, they enforce strict API protections, including multi-factor authentication and constant checks to verify each trade request (complete mediation). The bot runs with least privilege, only allowed to make specific, pre-approved types of trades. They also use explainability tools to monitor the bot's decisions, watching for any unusual patterns or signs of tampering that could indicate a security issue.

Phase five: monitoring and maintenance (NIST AI-RMF: GOVERN and MEASURE)

At this stage, the focus shifts to secure deployment and ongoing management of the AI system. Simply launching the model isn't enough – continuous monitoring and solid operational practices are essential to keeping it secure over time.

A key part of this is logging. By recording system and user activity, teams can investigate incidents, stay compliant and spot issues like data drift or data poisoning, where the AI's behaviour changes due to altered or corrupted input.

It's also important to keep systems updated. Developers must release security patches regularly, and operators need to make sure that these updates are applied. Big updates should always be followed by fresh security testing to check for new risks.

Another critical step is having a clear incident response plan, especially for AI-specific threats. Knowing how to detect, report and respond quickly can reduce damage from any security breach.

As AI models can learn and change over time, security has to be a continuous process. As models evolve, new issues can pop up – or old ones may return – making monitoring, patching and retraining essential.

And when it comes to data privacy, if a user asks for their data to be deleted (the 'right to erasure'), it may not be enough to just delete the file; you might also need to remove its influence from the model. This process, called 'unlearning', adds another layer to AI security: managing what the AI knows, and forgetting it when necessary.

All of these efforts work together in a feedback loop, where monitoring drives updates, retraining, and even unlearning to keep the AI system safe and reliable over time.

Example: A company uses an AI system to moderate online content. It constantly checks its own performance, looking for signs that it's letting harmful posts slip through or mislabelling content. One day, the system's accuracy drops suddenly – a red flag that could indicate a data-poisoning attack. An alert is sent to the security team, which kicks off the incident response plan. The model is then retrained using clean data, and the latest security updates are applied to restore safe and accurate performance.

ATTACK VECTOR	DESCRIPTION	PRIMARY LIFE CYCLE PHASE(S) AFFECTED	EXAMPLE (BRIEF)
DATA POISONING	Attackers inject malicious data into training sets to skew model behaviour or embed back doors	Data collection and preparation, model training, and evaluation	A content moderation AI unknowingly trains on data containing subtle patterns, later allowing harmful content
PROMPT INJECTION	Carefully worded inputs override safety measures or redirect AI behaviour	Deployment and inference	An AI assistant visits a website with hidden commands that modify shopping orders or reveal sensitive information.
MODEL DESERIALISATION	Malicious code embedded within packaged AI models activates when loaded	Model training and evaluation, deployment, and inference	A seemingly legitimate document (model) secretly installs malware when opened by an application
MODEL INVERSION	Attackers reconstruct sensitive training data by analysing model outputs	Deployment and inference	An attacker infers patient medical records from a healthcare diagnosis model's outputs
MODEL STEALING (EXTRACTION)	An attacker replicates a proprietary model's functionality by querying it and observing outputs	Model training and evaluation, deployment, and inference	A competitor replicates a fraud detection model to gain a competitive edge or misuse its capabilities
MEMBERSHIP INFERENCE	Attackers determine if a specific data record was used in a model's training set	Deployment and inference	An attacker deduces if an individual's sensitive health data was part of a synthetic dataset
LLMJACKING (RESOURCE HIJACKING)	Adversaries subvert AI infrastructure for unauthorised purposes like training malicious models or cryptomining	Deployment and inference, monitoring, and maintenance	Compromising an open-source AI model to deploy cryptocurrency miners on user systems
EXCESSIVE AGENCY	Autonomous AI systems execute harmful actions without sufficient oversight	problem definition and design, deployment and inference	An AI home assistant interacts with a fraudulent website, causing it to secretly order unauthorised items
ADVERSARIAL MISUSE OF OUTPUTS	Manipulating an AI system's legitimate outputs to craft adversarial examples that bypass security measures	Deployment and inference	An AI model is manipulated to produce inappropriate content, causing reputational damage
SUPPLY CHAIN COMPROMISE	Vulnerabilities in third-party AI components (datasets, frameworks, pre-trained models) are exploited	Problem definition and design, model training, and evaluation	Exploits targeting popular AI development libraries compromise integrated systems of many users

Table 1. Key AI attack vectors and their life cycle relevance

AI LIFE CYCLE PHASE	KEY SECURITY PRINCIPLES APPLIED	SPECIFIC EXAMPLE/ACTION	RELEVANT AI-SPECIFIC VULNERABILITY ADDRESSED
PROBLEM DEFINITION AND DESIGN	Security by design, least privilege, accountability, open design	Conduct AI-specific threat modelling using MITRE ATLAS to identify machine learning supply chain risks and plan for MLSecOps documentation	Machine learning supply chain compromise, model reconnaissance, exfiltration via machine learning inference
DATA COLLECTION AND PREPARATION	Confidentiality, integrity, data minimisation, privacy-enhanced	Implement differential privacy or federated learning for sensitive data; conduct fairness audits to detect and mitigate bias in training data	Data poisoning, privacy breaches, harmful bias
MODEL TRAINING AND EVALUATION	Integrity, robustness, defense in depth, secure by default	Apply adversarial training to enhance model resilience, rigorously test models against evasion and prompt injection attacks, and vet all third-party dependencies	Evasion attacks, prompt injection, model deserialisation, supply chain risks
DEPLOYMENT AND INFERENCE	Least privilege, complete mediation, secure by default, explainability	Deploy AI services with minimal permissions; continuously verify authorisation for all model interactions; implement post-hoc explainability tools to monitor decisions	Unauthorised access, model inversion, membership inference, excessive agency
MONITORING AND MAINTENANCE	Availability, accountability, continuous monitoring, incident response	Log system/user actions and analyse for anomalies (data drift, poisoning); provide regular security updates and patches; maintain an incident response plan	Data poisoning, model tampering, denial of service, unexpected behaviour

Table 2. Application of security principles across AI life cycle phases

LEVERAGING INDUSTRY FRAMEWORKS

Governments and global agencies are now creating detailed frameworks to help make AI systems more secure and trustworthy. These frameworks – like the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) from the United States, and ENISA's Multilayer Cybersecurity Framework from Europe – mark a big step forward in how AI security is handled. Instead of relying on one-off or informal efforts, these frameworks promote standardised, auditable processes that organisations can follow to reduce AI risks. They were created openly and collaboratively, showing a shared understanding that AI brings unique security challenges that need structured solutions.

While using these frameworks is still optional for now, they're closely aligned with upcoming regulations like the European Union AI Act – so they're helping industries get ready before stricter rules take effect. The growing influence of AI in society is driving this move toward formal, responsible practices that prevent harm and support innovation.

CONCLUSION: THE FUTURE OF TRUSTWORTHY AI

Building AI systems with security in mind from the start isn't a burden; it's what makes real innovation and trust possible. When organisations embed security into every stage of the AI life cycle – from the initial design to ongoing monitoring – they create systems that are stronger, more reliable, and better prepared to handle evolving threats. This proactive approach helps fix problems early, before they ever reach users, which builds confidence among customers and stakeholders.

AI security isn't something you do once and forget. As AI systems constantly learn and change, their security must also evolve. That's why continuous monitoring, regular updates and feedback loops are essential. In some cases, systems may even need the ability to 'unlearn' certain data to meet privacy or ethical requirements.

None of this works without strong leadership and a security-first culture. Leaders must make security a clear priority, and teams across development, operations and security must work together. With the right collaboration and mindset, organisations can safely tap into the full potential of AI, creating powerful tools that people can truly trust. ●

Rakesh Sharma is a seasoned cyber security and AI practitioner with more than 19 years of multidisciplinary experience across global financial institutions and cybersecurity product firms. Currently, he works as the Chief Advisor at CYAIFI, a cyber security and AI think tank. Sharma has led security efforts on cloud transformation programs across multiple organisations in the past. He is an Australian Information Security Association member and contributes to several community initiatives in ISACA, ISC2 and Cloud Security Alliance.

Stop blaming human error: it's time to focus on human response

BY JACQUELINE JAYNE, FRACTIONAL ADVOCATE FOR HUMAN-CENTRIC SECURITY, SOSAFE

CYBER SECURITY PROFESSIONALS have long leaned on a familiar explanation for many incidents: human error. We've called it the 'human element', the 'last line of defence', or even the 'human firewall' and 'the weakest link'. But no matter the label, the implication has always been clear: end users are the problem.

We trained them again and again. Simulated phishing and awareness modules. Created posters and newsletters. Held annual refreshers. Billions of dollars later, the data is in – the rate of human error in cyber incidents hasn't budged.

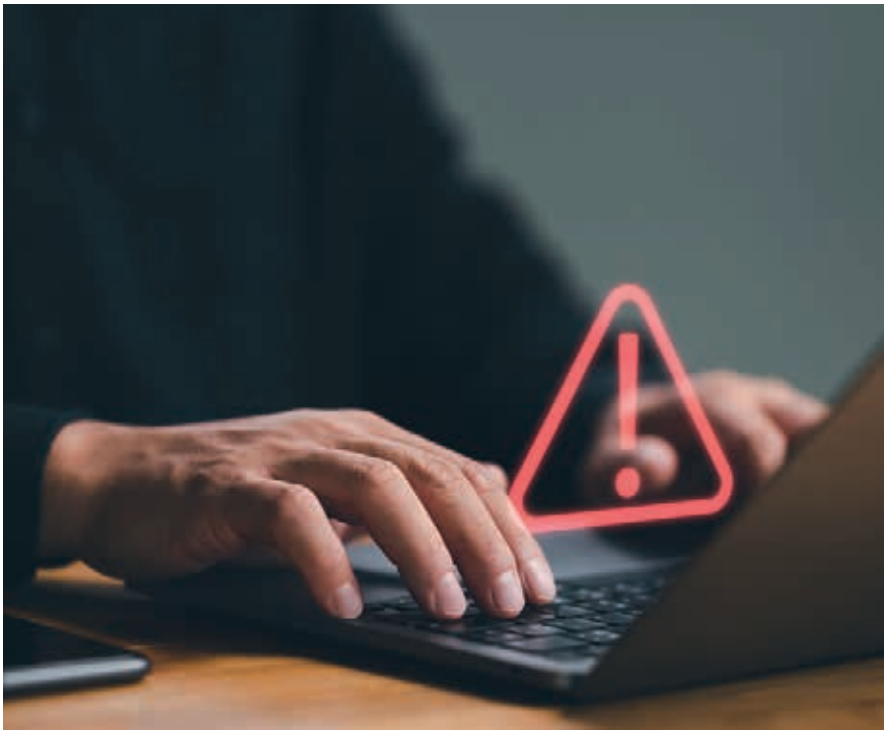
Despite increased investment in security awareness training platforms, the expected decrease in error rates hasn't materialised. If more training equalled fewer mistakes, we'd see it; but we don't.

The truth is uncomfortable: we've been focused on the wrong thing. Awareness alone doesn't change behaviour. Simulated phishing, on its own, doesn't build security-minded habits. Simply labelling people as the last line of defence or the weakest link ignores the complexity of human behaviour in moments of stress, urgency, fear, or even boredom.

Let's be clear: cyber security is a human issue; however, we still act as if technology will solve the problem. We deploy tools to catch what people miss, instead of understanding why they missed it in the first place.

Now, a growing number of organisations are making real progress in reducing human risk. What's different? They aren't throwing out training and phishing simulations; they're putting them into context – shifting the focus from addressing 'human error' to addressing 'human response'.

Human response is the new frontier. It's about recognising that most attack vectors only succeed when a person responds – not logically, but emotionally. Phishing, business email compromise, romance scams and ransomware all exploit the human brain's decision-making shortcuts. To combat this, we need to understand those responses, and address them with the same rigour we apply to firewalls and endpoint protection.



Jacqueline Jayne

Behavioural science and psychology are not 'nice to haves' in security; they are essential. When we understand why people click, respond, download or share, we can design better interventions – ones that reduce real risk.

It's not about fixing people; it's about designing environments, cues, and cultures that support better decision-making under pressure. By applying principles such as cognitive load reduction, habit formation and emotional regulation, we can design systems that work in harmony with human nature, rather than against it. This is how we shift from simple awareness to true behavioural change.

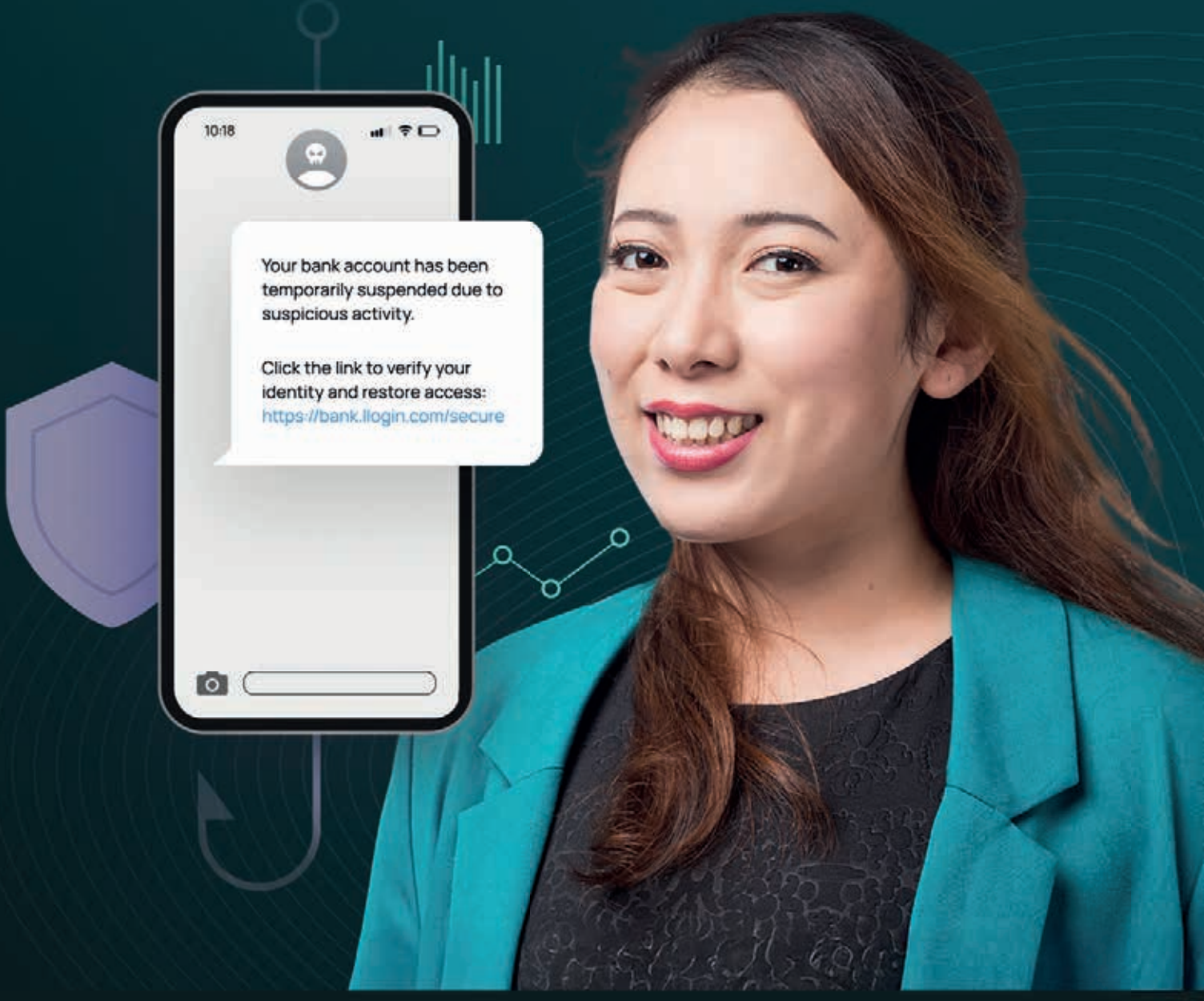
If cybercriminals are focusing on human response, why aren't we? It should be the first vector of opportunity for both attackers and defenders.

If we genuinely want to manage human risk, it's time to stop blaming errors, and start understanding and addressing responses. •

Jacqueline Jayne is a consistent and trusted voice in the evolving cyberthreat landscape, shaping how businesses address human error and security awareness programs. In addition to media commitments and speaking engagements, she currently serves as Advocate for Human-Centric Security at SoSafe (sosafe-awareness.com).

sosafe

YOUR PARTNER IN
HUMAN-FIRST DIGITAL DEFENCE



One click changes everything

We help your team **stay safe and prepared** with cyber security training that **empowers them** to spot risks and take smart actions.

sosafe-awareness.com

→ Scan the QR code and empower your people to stay secure!

Securing the AI Revolution: Why Identity is Your Mission-Critical Defense

> “The journey to ensure that you have a fully baked identity security strategy is long, but getting started is the most important part.”
>
> **Mathew Graham**
> Regional Chief Security Officer Asia Pacific, Okta

Download
Okta Identity Maturity Model

The rapid proliferation of AI agents and automated services has ushered in a new era of productivity and efficiency for businesses. However, this revolution presents a significant challenge for security leaders - how to secure non-human identities without stifling innovation. The key to navigating this new landscape with confidence is a proactive and mature identity security strategy.

The traditional security model, which often relies on static service accounts, is no longer sufficient. These high-privilege accounts are a prime target for bad actors, and a single compromised credential can open the door to an organisation's most sensitive data. The solution lies in a more intelligent approach—one that treats every identity, human or non-human, as a potential risk.

Okta’s vision is to establish an **identity security fabric** that secures every identity in the enterprise **before, during, and after authentication**. This independent and neutral fabric is a holistic, end-to-end orchestration of access management, governance, and privileged access management. A crucial component of this fabric is **Cross-App Access**, an evolution of the OAuth standard. Instead of using vulnerable service accounts, this method allows applications to define precise access levels through a central identity provider. This not only enhances security by limiting an agent's permissions to only what's necessary but also simplifies the user experience by eliminating constant and disruptive consent prompts.

Beyond AI, a mature security strategy must also address persistent threats like identity misconfigurations, phishing, and post-authentication attacks. Okta’s **Identity Security Posture Management** product provides crucial visibility into potential misconfigurations, while **Okta FastPass** offers a robust, phishing-resistant authentication method that performs advanced device posture assessments. To combat the growing threat of session cookie theft, Okta's AI-driven risk engine continuously analyses signals and can take real-time actions, such as logging a user out and destroying session cookies, to protect against post-authentication attacks.

Building a comprehensive identity security strategy can feel daunting, but the most important step is simply to begin. As Mathew Graham, APAC CSO at Okta, states, "The journey to ensure that you have a fully baked identity security strategy is long, but getting started is the most important part." This could mean something as fundamental as moving beyond phishable MFA factors or being more proactive with identity security posture management. By prioritising identity as a mission-critical component of your security strategy, you can confidently embrace the AI revolution while building a resilient and future-proof defense against modern threats.

Next Steps

Ready to assess your organisation's identity security? Download The **Okta Identity Maturity Model** to understand where you stand and what steps you can take to build a more secure and resilient foundation.

AI, secured: Powering trust and innovation

Identity-first security manages access, mitigates risk, and drives trusted digital experiences

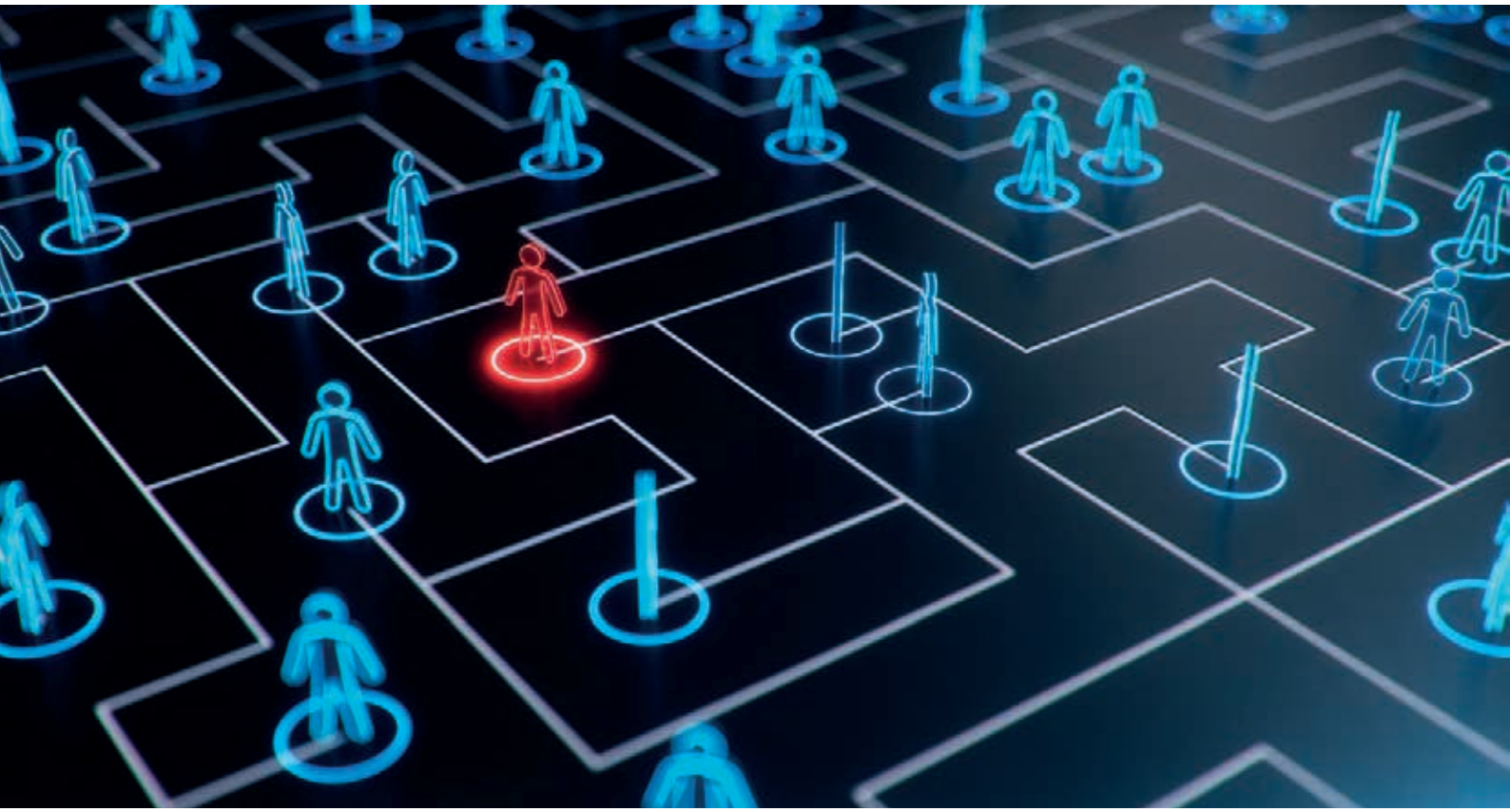
okta
The World's Identity Company™

Learn more at okta.com/au

DECODING EXTREMIST CONTENT WITH LANGUAGE MODELS

BY DR CHRISTINE DE KOCK

Artificial intelligence can lighten the load for moderators, but human judgement remains essential.



The recent Netflix miniseries *Adolescence* centres on incels: a particularly toxic and violent online anti-women group. Such has been the impact of the show that its creators were invited to discussions with United Kingdom's Prime Minister Keir Starmer on the topic of online safety for young people.

Closer to home, the Australian Security Intelligence Organisation has singled out the particularly concerning violent extremist ideology held by incels. While incels primarily interact online, their impact translates into real-world violence: the 2024 Bondi mass stabbing attack has been linked to, and claimed by, the incel community. Recent developments in artificial intelligence (AI) might support large-scale monitoring of online content for such risks, but it is not without vulnerabilities.

CODED LANGUAGE

In the second episode of *Adolescence*, a teenager explains to a police officer that innocuous-seeming Instagram comments are, in fact, recognised in-group language within the incel ecosystem. Ranging from too subtle to notice to completely unintelligible, in-group language serves two important social roles in groups: first, it signals cohesion and solidarity with a group by illustrating an awareness and acceptance of their norms; and second, it can obscure the discussions of the group from out-group onlookers. The latter highlights a key challenge in moderating extremist content: although communication may occur on public platforms, it tends to be obfuscated, such that it can be near-impossible for non-group

members to accurately decode. Examples of this are shown in Figure 1, along with attempts by a language model to 'translate' them. Of particular note is the term 'going ER', which refers to committing a mass murder. This is not correctly interpreted by the language model, indicating that there are limitations to using AI models for the automated moderation of extremist content.

WHY IS IT DIFFICULT?

The recent excitement around language models can, to a large degree, be attributed to their capacity for 'emergent behaviour', or an ability to master tasks without being explicitly trained to do them. This is achieved through exposure to large amounts of unstructured text data and advanced learning algorithms. As per the classic garbage in, garbage out (GIGO) principle, the data that goes into training these models are a key determinant of their performance. Many of the leading models are trained on datasets that were explicitly selected to exclude hateful and toxic content. That means that general-purpose language models are less suited to tasks like moderating hate speech and extremist content.

Another significant challenge is the fact that the language used in the incel community is very dynamic, developing at a much higher rate than what has been observed in other extremist groups. Current language models are not designed to accommodate the temporal evolution of language. Furthermore, the training data naturally has a time horizon, meaning that recent developments would not be captured by slightly out-of-date models.

WHAT CAN WE DO?

In a recent series of papers, we explore the question of how AI can be used to address these threats. One of these studies evaluates a range of large language models (LLMs) on the task of providing definitions for 400 known instances of incel in-group language. Our motivation in this task is twofold. Firstly, we are interested in probing how well these models capture this non-standard language, given that they may not be trained on the right data. Secondly, we would like to establish the feasibility of using LLMs to provide definitions of unknown terms for human moderators who monitor these groups for potential threats.

We provide two test settings: providing only a word (referred to as the base setting), and providing the word plus examples of its usage in the incel community. Model outputs are validated by a human expert – a sociologist who specialises in incels. Our findings show that the best model obtains an accuracy of 46 per cent for the base setting, which rises to 88 per cent when provided with contextual examples.

Figure 1. Three posts from our dataset (in gray) with translations by Llama-3.3-70B-Instruct (in green). The posts originate from incels.is (1 and 2) and storm-front.org (3)

The low initial accuracy indicates that, as we expected, the model is unfamiliar with a lot of the terminology; however, when provided with example usages, it can infer its meaning based on context – much like a human would do.

This simple experiment provides an instructive example on the application of LLMs in domains for which they may lack training data: where data is scarce, poor performance may result; however, this can potentially be remedied by providing additional information. The results indicate that, under specific conditions, LLMs can provide useful tools to support human moderators in monitoring online discussions; however, as shown in the 'going ER' example, subtle but crucial nuances may still be missed, meaning that this is not yet a job that can be fully outsourced to the bots. •

Dr Christine de Kock is a faculty member in the School for Computing and Information Systems at The University of Melbourne, conducting research on online communities by using AI and natural language processing. Before joining The University of Melbourne, de Kock completed a PhD in Computer Science at Cambridge University.

Data-first security: why exposure management trumps good luck

BY ANDREW PHILP, ANZ FIELD CISO, TREND MICRO

WHEN TREND MICRO set out to understand what really drives cyber carnage, we didn't start with assumptions. We watched 190 organisations in the wild and measured actual, observed damage, logging every confirmed exfiltration or operational impact mapped to the MITRE ATT&CK framework. The findings weren't hypothetical; they were real, and they were stark.

What our telemetry data showed us was that organisations with high rates of exposure to cyber risks are 2.6 times more likely to suffer damaging attacks. Even with a managed detection and response (MDR) service in place, the reduction in incident rate was modest – just a dip from 42 per cent to 33 per cent. But when low exposure is paired with MDR, the damage rate plummets to 13 per cent.

The message is clear: exposure management is the lever that truly shifts outcomes. Attackers don't need to be clever if your estate is easy to exploit. Proactive security doesn't begin with faster alerts – it starts with fewer openings. The less there is to target, the less there is to breach. That's how you build cyber resilience before the next attempt arrives.

Security teams need to turn exposure into a modifiable control point. Continuous cyber risk exposure management (CREM) is the lever that makes this possible, offering a living map of weaknesses rather than a static point-in-time audit. With this view, teams can prioritise remediation based on business impact, not just CVE scores.

Engineering for containment also matters. The CREM lens helps cyber security operatives to rehearse for impact. When incidents do happen, MDR teams armed with that context can isolate fast, with decisiveness. And when exposure is low to begin with, attackers move slower, giving the security operations centre (SOC) more room to manoeuvre.

Making exposure metrics part of the board conversation is critical, as well. For instance, Trend Micro's Exposure Index, which gauges organisations' vulnerability to cyberthreats, is designed not just for analysts, but for CFOs and directors, too. When you can show how lower scores correlate with fewer incidents, cyber security becomes a business enabler.

Finally, it's important to recognise that this isn't something that every team can solve internally. Cyber risk advisory services, and managed extended detection and response bring outside perspective, helping organisations with stretched resources to get fast wins and chart a maturity road map. This way, progress can be measured, managed and repeated.

The bottom line for CISOs in Australia is this: outsourcing detection while ignoring exposure is like hiring lifeguards, but leaving the pool gate open. Our data proves it. Risk exposure is one of the strongest predictors of whether a cyber attack causes damage. Start where the attacker starts – at the point of entry.

The old maxim 'prevention is better than cure' has long been a favoured philosophy in the cyber security landscape, and cyber risk exposure management is the best approach to ensure that a strong security posture isn't left to luck. Nail this, and every dollar spent on detection, response and analytics will go further. •


TREND MICRO™
Global Leader in Cybersecurity
Proactive security starts here
Your path to innovation starts with an enterprise cybersecurity platform.
One that centralises risk management, security operations, and layered protection.
One that achieves a 92%* reduction in ransomware risk.
Turn security into your innovation catalyst with Trend Vision One™.
See what's possible at TrendMicro.com/visionone
*From Vulnerable to Resilient: Cutting Ransomware Risk with Proactive Attack Surface Management, Bakuei Matsukawa, 2024
©2025 Trend Micro, Inc. All rights reserved

Security should be uncomfortable – that's the point

BY MALHAR VORA, PAM ENGINEERING LEAD, SME AND PEOPLE LEADER, ANZ BANK

In a world obsessed with making everything effortless – where apps and services anticipate our every whim – a vital truth in cyber security often gets lost: true security, deep down, needs to feel a little uncomfortable. This isn't about arbitrary roadblocks or making digital lives harder just because we can. It's about designing smart, intentional friction that keeps us safe.

We're all used to frictionless user experiences – one-click logins, autofill, the expectation that technology just gets us. While convenient in many areas, in digital security this ease can lull us into dangerous complacency. It creates easy paths for bad actors and often encourages us to be less careful. It's time to gently challenge this comfortable status quo.

THE QUIET GUARDIANS: INTELLIGENT FRICTION IN CYBER SECURITY

Think of security not as a brick wall, but as a series of friendly, intelligent checkpoints. They're not there to annoy you, but to prompt a moment of awareness – a small pause that makes a huge difference. Let's explore how the subtle 'discomfort' of common cyber security measures are actually a powerful act of protection.

IDENTITY AND ACCESS MANAGEMENT: YOUR DIGITAL KEYS

Identity and access management is the bedrock of digital security, controlling who accesses what. Friction here is about verification and limitation.

Multi-factor authentication: the guardian's gentle nudge

We've all grumbled about having to grab our phone for that second code, but that quick grab – that tiny extra step – transforms a simple login into a conscious act. It's your personal safeguard against stolen credentials, and is remarkably effective. Multi-factor authentication's slight inconvenience forces a momentary break from autopilot, making you a proactive participant in your own security, and preventing automated attacks.

Strong passwords (and the shift to passwordless): redefining effort

Remember the frustration of creating a 'strong' password? It felt like an irritating chore. Now, with passwordless solutions like biometrics or hardware keys, there's a new 'uncomfortableness': the initial effort of set up and trusting a new login method. This temporary hurdle leads to a vastly more secure and, eventually, convenient digital life, shifting the burden from human memory to secure hardware.

Granular access controls (RBAC/ABAC): precision over permissiveness

Ever wonder why you can't access a certain file? This comes from specific access rules that limit you to precisely what your job requires. It feels restrictive, yes, but it's a critical safety net, preventing accidental exposure or malicious lateral movement if an account is compromised. It protects both data and you from unintended consequences, ensuring that users operate within tightly defined boundaries.

PRIVILEGED ACCESS MANAGEMENT: GUARDING THE CROWN JEWELS

Malhar Vora

For those managing our most critical systems, privileged access management is a necessity that definitely adds friction. It's designed to make life harder for the most powerful accounts, as their compromise has the highest impact.

Just-in-time access: the temporary key

Admins don't just have elevated access; they ask for it, for specific tasks, for limited times. This extra step feels like a burden, but it dramatically shrinks the window an attacker has to exploit powerful credentials. This 'just in time' friction ensures that privileged accounts are elevated only when necessary, making them less attractive targets.

Think of security not as a brick wall, but as a series of friendly, intelligent checkpoints. They're not there to annoy you, but to prompt a moment of awareness ...

Session monitoring: the visible eye

Knowing that privileged actions are recorded can feel a bit like Big Brother is watching. This constant oversight can be uncomfortable. But in a breach, this 'intrusion' becomes an invaluable road map for understanding what happened, minimising damage and stopping future attacks. It provides a powerful disincentive against malicious activity and an indispensable forensic trail.

Password vaulting: the abstracted control

Not knowing the 'root' password directly – having it managed by a secure vault – is a big shift. It changes the workflow and can feel less intuitive. Yet, this abstraction is a powerful defence, preventing those 'keys to the kingdom' from falling into the wrong hands. It adds a controlled, audited layer of access, reducing credential theft risk.

IDENTITY GOVERNANCE AND ADMINISTRATION: THE INVISIBLE SCRUTINY

Identity governance and administration is the often invisible guardian that feels like 'paperwork' for managers, but is truly foundational, addressing identity and permission life cycles.

Access reviews: the periodic housekeeping

Periodically, managers review and confirm who on their

team still needs access to what. It's an administrative task that pulls you from other duties; however, this 'burden' catches orphaned accounts, prevents former employees from retaining access, and stops permissions from quietly growing into massive security risks. This regular, often tedious process is essential for maintaining least privilege.

Segregation of duties: the collaborative hurdle
Imagine a system preventing one person from approving a payment and then releasing the funds. It adds steps, perhaps even requiring another colleague – but this 'friction' is a deliberate design to prevent fraud and human error, protecting the organisation's financial integrity. Segregation of duties introduces necessary bureaucratic friction, requiring multiple individuals for sensitive tasks.

PROTECTING YOUR DIGITAL WORKSPACE AND DATA

Beyond identity, the devices and data we interact with daily also benefit from intelligent friction.

Endpoint detection and response: the constant sentinel
You might occasionally notice a slight slowdown or wonder why IT monitors your computer so closely. This constant, pervasive monitoring by endpoint detection and response agents can feel intrusive; however, this 'intrusion' allows security teams to catch sophisticated attacks that a traditional antivirus misses. It's the early warning system protecting your work and data. The subtle friction is the cost of comprehensive, real-time threat detection.

Data loss prevention: the protective barrier
Suddenly, you can't email that large file to your personal drive, or upload a document to a new cloud service. It can feel like the system unnecessarily blocks your flow. But this 'friction' is data loss prevention doing its job: stopping sensitive company or customer data from accidentally (or intentionally) leaving the secure perimeter, helping to meet compliance and prevent costly breaches.

Software restriction policies/application whitelisting: the curated environment
Being told you can't install certain software, even if you think it helps your job, can be frustrating – it limits your choices. But this 'discomfort' is a powerful

defence against malware and vulnerabilities from unapproved applications, creating a much safer computing environment. The friction here is a constraint on user autonomy, significantly reducing the attack surface.

NUDGING TOWARDS SAFER HABITS

Beyond technical controls, intelligent friction can be designed to influence human behaviour, often the weakest link in security.

Network segmentation: the compartmentalised world

Ever found yourself unable to access a network resource that used to work? This comes from network segmentation, limiting connections to only what's essential. It can be a minor annoyance when you need access beyond your usual scope. Yet, this architectural friction is invaluable in containing a breach, preventing an attacker from easily moving through the entire network.

Contextual/adaptive authentication: the risk-aware challenge

Most of the time, this is seamless; but if you try to log in from a new country, a strange device, or at 3 am, the system might suddenly ask for extra verification. This unexpected discomfort is security kicking in when risk is highest, stopping potential attackers by demanding extra proof that it's really you.

Security awareness training and phishing simulations: the habit builders

Yes, mandatory training takes time, and getting caught by a simulated phishing email can feel embarrassing; but these regular, sometimes uncomfortable, exercises are crucial. They build your digital muscle memory, turning you into a more vigilant human firewall against common attacks. It's an investment in your personal security, and the organisation's security.

THE UNCOMFORTABLE TRUTHS FOR AUSTRALIAN ORGANISATIONS

Australia faces unique cyber security challenges: critical infrastructure targets, increasing digitisation, and remote work reliance that can lack adequate controls. This makes 'intelligent friction' even more pertinent.

For Australian CISOs and security teams, advocating for these 'uncomfortable' measures often means navigating internal resistance. The push for 'seamless' user experience is strong, driven by productivity and user satisfaction; however, the cost of a breach – from regulatory penalties under the Privacy Act, to reputational damage – far outweighs the minor discomfort of robust security controls. Embracing intelligent friction requires a cultural shift, moving beyond check box compliance to genuine commitment. It means educating stakeholders – from the board to the end user – that a little friction isn't poor design, but rather a hallmark of resilience.

EMBRACING THE UNCOMFORTABLE, TOGETHER

When security asks us to pause, take an extra step, or learn a new process, it fosters vital accountability. It makes us ask questions, like: 'Am I sure I want to click this?' and 'Is this really the right way?' This continuous, subtle reinforcement helps us to:

- prevent attacks by making it genuinely harder for cybercriminals
- reduce risky behaviour by gently nudging us towards safer digital habits
- boost awareness through every small moment of 'discomfort' – each one is a tiny lesson, reinforcing security's importance.

As cyber security professionals, our goal isn't to make people's digital life miserable. It's to design experiences where security is a logical, necessary part of interacting with technology. This requires a shift in how we all think – from security professionals designing systems, to every individual user. For us, it means prioritising robust protection even when it means sacrificing immediate 'seamlessness'. For the user, it means understanding that a small moment of discomfort is a tiny price for your data's integrity and your organisation's resilience.

Let's embrace this productive discomfort. As Australian security professionals, we have a unique opportunity to lead this conversation, championing a future where security isn't just an invisible layer, but a deliberate, valued, and ultimately empowering part of our digital lives. Let's make security feel a little more uncomfortable, for all the right reasons. ●

Malhar Vora is an accomplished professional and seasoned expert in privileged access management (PAM), and identity and access management, boasting more than 19 years of extensive experience. He specialises in large-scale cyber security implementations across on-premises and public cloud environments, driving secure, scalable, and innovative solutions. As PAM Engineering Lead, SME and People Leader at ANZ Bank, Vora leads a high-performing team of CyberArk engineers. His role encompasses the full life cycle of PAM systems, from solution design, development and testing, to complex global implementations and continuous innovation through automation. Notably, he excels in cloud PAM deployments, leveraging CI/CD tools like Ansible, Terraform and CodeFresh for efficient outcomes, and has delivered enterprise security solutions across Australia, New Zealand, and the United Kingdom.

Train, retain, perform

Building cyber security resilience through workforce development with SANS.

TODAY'S CYBER SECURITY leaders face a dual challenge: escalating threatsa nd a widening skills gap. Recruiting talent alone is no longer enough; roles can take months to fill, are costly, and often don't guarantee the expertise needed to secure complex environments. What organisations need is not just more staff, but better-trained teams. That's where a deliberate strategy of 'train, retain, perform' delivers measurable impact.

TRAINING: BUILDING SKILLS THAT STICK

Hiring externally can be expensive and slow. On average, cyber security positions take 3–6 months to fill, and a single bad hire can cost up to $35,000. By contrast, targeted training develops capabilities faster and more effectively. According to SANS research, 52 per cent of organisations say a lack of the right skills is a bigger concern than a lack of headcount. Training addresses this directly.

Equally important is how professionals learn. Traditional lectures result in just five per cent knowledge retention, whereas hands-on, scenario-based training enables learners to retain up to 75 per cent. More than half of cyber security professionals prefer this interactive style, which builds instincts essential for responding under pressure. Teams trained through these immersive methods report higher satisfaction, stronger engagement and greater long-term performance.

RETENTION: INVESTING IN PEOPLE PAYS OFF

The cyber security job market is competitive, and retention is just as critical as recruitment. Employees who feel supported through continuous learning are more likely to stay and to thrive. Formal training and certification programs signal that organisations value professional growth, and data shows that 65 per cent of organisations now require certification for client-facing roles. This emphasis not only strengthens security posture, but also helps to retain skilled practitioners in an industry where burnout and turnover are common.

Retaining talent is also a matter of financial prudence. International Data Corporation's (IDC's) research shows that SANS-trained employees deliver $52,700 in annual value each, while helping organisations to avoid nearly $125,000 in hiring costs every year. Training isn't just a benefit for employees; it's a clear business case.

PERFORMANCE: STRONGER TEAMS, MEASURABLE RESULTS

The return on training is not theoretical; it is quantifiable. IDC's study found that organisations with SANS-trained staff saw 4.2 times faster threat identification and 51.6 per cent faster incident response. The result? An average annual value of $3.57 million delivered per organisation. In addition, training reduced reliance on external vendors (saving nearly $900,000 annually) and prevented close to $1 million in fraud damage each year.

These outcomes reinforce a simple truth: high-performing cyber security teams aren't built by expanding headcount alone. Instead, they are built by investing in the people already in place, equipping them with the skills and confidence to meet modern threats head-on.

CONCLUSION: A SMARTER PATH FORWARD

Cyber security resilience doesn't come from chasing scarce talent; it comes from cultivating it. By committing to a 'train, retain, perform' approach, organisations create teams that are not only technically proficient, but also motivated, engaged and ready to defend against evolving risks. •

For more information on how SANS can support your organisation in strengthening cyber resilience with training and certifications, email ANZ@sans.org or call +61 2 6174 4581.

Findings cited from: IDC White Paper, Sponsored by SANS Institute, 'The Business Value of SANS'.

SANS

Train. Retain. **Perform.**

Headcount Doesn't Produce **High-Perfoming Teams**

Strong security teams aren't built by adding more people.
They're built by investing in the right ones.

52%

of organisations say "*not having the right staff*" is a bigger concern than lack of personnel

55%

of organisations now run formal cybersecurity training programs

65%

of organisations require cybersecurity certification for client-facing roles

Source: *SANS | GIAC 2025 Cybersecurity Workforce Research Report*

Hiring is Expensive. **Training is Smarter.**

ANZ Limited Time Offer

Receive Up To 30% Off SANS Courses. Unlock the World's Most Trusted Cyber Training, Now More Accessible Than Ever.

Until 31 December 2025, Enterprises and Government organisations in Australia and New Zealand can access SANS' world-class cybersecurity training with savings up to **AUD 4,005.**

Build foundational skills or advance into specialised roles with flexible training formats: In-Person, Virtually, or OnDemand.

The Offer

- **LEVEL 300 & 400 COURSES**
  30% discount (up to $4,005) to the course price
- **LEVEL 500 COURSES**
  20% discount (up to $2,670) to the course price

This offer is not valid with any other promotions.
SANS Voucher customers, get in touch with us to discuss available options

Eligible Australia based events

- **SANS Brisbane**
  13-18 October 2025
- **SANS Canberra November**
  3-8 November 2025

ACT NOW , don't miss this opportunity to equip your team with elite cybersecurity skills and stay ahead of threats

For more information, email us at **anz@sans.org** **www.sans.org** **+61 2 6174 4581**

What if we designed cyber security like urban planners, not police officers?

BY MARYAM SHORAKA

Reimagining security as civic infrastructure – like roads and water – invites more inclusive, proactive, and human-centred models.

Maryam Shoraka

Standing in the security operations centre at 2 am, watching another incident unfold across multiple screens, I found myself thinking about my morning commute through Sydney's CBD. The traffic flows seamlessly through carefully designed intersections, pedestrians cross safely at designated points, and the entire system hums along despite accommodating millions of daily interactions. Yet, here I was, once again playing digital detective, chasing threats through our networks like a constable pursuing criminals through dark alleys.

This moment crystallised a fundamental question that has been brewing in cyber security circles: What if we've been approaching security all wrong?

THE POLICE OFFICER'S DILEMMA

For decades, cyber security has operated under what I call the 'police officer paradigm'. We patrol digital perimeters, investigate incidents after they occur, and chase bad actors through increasingly complex digital landscapes. Our language betrays this mindset – we speak of threat hunting, incident response and forensic investigations. We build walls, deploy guards, and respond to breaches with the urgency of emergency services racing to a crime scene.

This approach has served us well in many respects. The Australian Cyber Security Centre's Annual Cyber Threat Report 2024 shows that Australian organisations reported more than 94,000 cybercrime incidents, averaging one report every six minutes. The traditional security model has undoubtedly prevented countless more attacks and minimised damage from successful ones. But here's the challenge: despite billions of dollars invested in cyber security globally, breaches continue to rise, and the human cost of our reactive approach is becoming unsustainable.

Consider the typical security incident response: a breach is detected, teams are mobilised, systems are locked down, and users find themselves locked out of critical applications while forensic investigations commence. The focus shifts entirely to catching the perpetrator and understanding what went wrong. Meanwhile, business operations grind to a halt, productivity plummets, and employees feel like suspects in their own workplace.

A financial services executive I worked with recently captured this perfectly: 'Every time we have a security incident, it feels like our office becomes a crime scene. People stop collaborating, stop innovating, and start looking over their shoulders. We solve the immediate problem, but we're slowly killing the culture that makes our business successful.'

LEARNING FROM THE URBAN PLANNER'S TOOLKIT

Urban planners approach city design with a fundamentally different philosophy. They don't wait for traffic accidents to happen before designing safer intersections. Instead, they study traffic patterns, understand human behaviour, and design infrastructure that naturally guides people towards safe, efficient outcomes. They think in systems, not incidents.

When Melbourne's urban planners redesigned the city's laneways in the 1990s, they didn't increase police patrols or install more security cameras. Instead, they introduced mixed-use development, improved lighting, and created natural gathering spaces. Crime decreased not because enforcement increased, but because the environment itself discouraged antisocial behaviour while encouraging positive community interaction.

This systemic thinking offers profound lessons for cyber security. What if, instead of waiting for attacks and then responding, we designed digital environments that naturally guided users towards secure behaviours while making life difficult for attackers?

INFRASTRUCTURE THINKING FOR DIGITAL SECURITY

The infrastructure model suggests treating cyber security like we treat roads, water systems, or electrical grids – as essential civic infrastructure that enables society to function. This shift in perspective opens up entirely new approaches to security challenges.

Take user authentication, for example: traditionally one of our most friction-heavy security controls. The police officer's approach gives users complex password requirements, forces regular changes, and locks accounts after failed attempts. It's digital stop-and-frisk, making everyone prove they belong.

An infrastructure approach might look more like Sydney's Opal card system. Commuters tap on and off public transport seamlessly, with the system handling complex fare calculations, fraud detection, and network optimisation in the background. Users experience convenience and efficiency, while the system maintains security through elegant design rather than obvious controls.

Microsoft's research into passwordless authentication reflects this thinking. By moving towards biometric and device-based authentication, they're creating systems that are both more secure and more user-friendly – much like how contactless payment systems eliminated the friction of cash transactions while actually improving transaction security.

THE HUMAN-CENTRED SECURITY REVOLUTION

Perhaps the most profound difference between the police officer and urban planner models lies in their view of people: police officers see potential criminals; urban planners see citizens whose needs must be understood and accommodated.

Traditional cyber security often treats users as the weakest link in the security chain. We subject them to mandatory training, monitor their behaviour for anomalies, and blame them when things go wrong. It's a fundamentally adversarial relationship that creates resentment and drives shadow IT adoption.

The Australian Bureau of Statistics' 2023 Digital Inclusion Index revealed that 2.5 million Australians still lack basic digital skills. Yet, our security models often assume universal digital literacy and punish those who struggle with complex security protocols. This isn't just inequitable – it's strategically short-sighted.

Urban planners understand that effective infrastructure must work for everyone, from eight-year-

olds walking to school to 80-year-olds accessing essential services. They design for the full spectrum of human ability and behaviour. Security infrastructure should operate by the same principles.

Consider how Brisbane's Cross River Rail project approached accessibility. Rather than retrofitting accessibility features after construction, they embedded inclusive design from the beginning. The result is infrastructure that works better for everyone, not just those with specific accessibility needs.

BUILDING RESILIENT DIGITAL COMMUNITIES

Urban planners don't just design individual buildings; they create communities that can adapt and thrive over time. They understand that resilience comes not from impenetrable barriers, but from distributed systems that can absorb shocks and continue functioning.

This community thinking transforms how we approach cyber security. Instead of focusing solely on preventing breaches, we can design systems that assume breaches will occur and ensure they don't cascade into system-wide failures.

The 2022 Medibank cyber attack affected 9.7 million customers – nearly 40 per cent of Australia's population. While the breach was devastating, it highlighted the importance of system design. Organisations with proper data segmentation, encrypted backups, and incident response procedures were able to maintain operations and protect customer data even when parts of their systems were compromised.

Jane Morrison, who led the cyber security response for a major Australian retailer during a recent incident, described the difference: 'We stopped thinking about preventing every possible attack and started thinking about building systems that could fail safely. When we did get hit, our customers barely noticed because we'd designed redundancy and isolation into everything we built.'

The 2022 Medibank cyber attack affected 9.7 million customers – nearly 40 per cent of Australia's population. While the breach was devastating, it highlighted the importance of system design

PROACTIVE DESIGN PRINCIPLES

Urban planners use zoning laws, building codes and infrastructure standards to create environments that naturally promote desired outcomes. Similarly, cyber security can embed security principles into the fundamental design of digital systems.

The concept of 'security by design' isn't new, but implementing it requires thinking like an urban planner rather than a police officer. Instead of adding security controls to existing systems, we need to architect security into the foundational elements of our digital infrastructure.

Australia's Digital Transformation Agency's approach to government digital services exemplifies this thinking. Its design standards embed security, accessibility and usability as co-equal requirements from the project's inception. The result is government services that are simultaneously more secure and more user-friendly than their predecessors.

ECONOMIC MODELS AND SHARED RESPONSIBILITY

Urban infrastructure operates on models of shared investment and collective benefit. Roads, utilities and public transport are funded collectively because their benefits extend beyond individual users to society as a whole.

Cyber security suffers from misaligned incentives. Individual organisations bear the full cost of security investments, while the benefits of improved security posture extend to partners, customers and the broader digital ecosystem. This leads to systematic underinvestment in security infrastructure.

The Australian Government's Cyber Security Strategy 2023–2030 recognises this challenge, proposing shared responsibility models where government, industry and civil society collaborate on security infrastructure. The strategy specifically mentions treating cyber security as 'a collective responsibility' similar to public health or environmental protection.

Some Australian organisations are already experimenting with collaborative security models. The Australian Financial Services Information Sharing and Analysis Centre enables banks and financial institutions to share threat intelligence in real time, creating a distributed early warning system that benefits all participants.

Cyber security suffers from misaligned incentives. Individual organisations bear the full cost of security investments, while the benefits of improved security posture extend to partners, customers and the broader digital ecosystem

MEASURING SUCCESS DIFFERENTLY

Urban planners measure success through metrics like traffic flow efficiency, public space utilisation and citizen satisfaction scores. They focus on system performance and community outcomes, not just incident statistics.

Cyber security metrics, by contrast, often reflect the police officer mindset. We count threats detected, incidents responded to and vulnerabilities patched. These metrics tell us how busy our security teams are, but say little about whether our digital infrastructure is actually supporting business objectives and user needs.

Infrastructure metrics might include user productivity rates, system availability during security events, and the time required for legitimate users to access resources. These metrics would shift focus from security theatre to security effectiveness.

Dr Katina Michael from the University of Wollongong's research on cyber security metrics suggests that organisations measuring user experience alongside security outcomes achieve better results in both domains. 'When you optimise for security and usability simultaneously,' she notes, 'you often discover solutions that wouldn't emerge from optimising either dimension alone.'

IMPLEMENTATION CHALLENGES AND OPPORTUNITIES

Transitioning from the police officer to the urban planner model isn't without challenges. Existing security tools, processes, and organisational structures are built around incident response and threat hunting. Regulatory frameworks often mandate specific controls rather than outcomes, making innovative approaches difficult to implement.

Several trends, however, are creating opportunities for this transformation. Zero Trust architecture, which assumes no implicit trust based on network location, aligns naturally with infrastructure thinking. Cloud-native security services enable security capabilities to be embedded into development workflows rather than bolted on afterwards. Artificial intelligence and machine learning are making it possible to provide personalised security experiences that adapt to individual user contexts and risk profiles.

The key is starting small and building momentum. Organisations can begin by identifying high-friction security processes and redesigning them using infrastructure principles. Password policies, access request procedures and security training programs are all candidates for urban planner–style redesign.

A VISION FOR THE FUTURE

Imagine a digital workplace where security is as invisible and effective as the water system in your home. Users authenticate seamlessly by using biometric or device-based systems. Applications automatically adapt their security posture based on context and risk. Data protection happens transparently in the background. When security incidents occur, they're contained and remediated without disrupting business operations.

This isn't utopian thinking – it's infrastructure thinking applied to cyber security. Some organisations are already moving in this direction. Google's BeyondCorp initiative treats corporate network access

like internet access – no inherent trust based on location, with every access request evaluated based on comprehensive context. The result is better security with improved user experience.

Similarly, companies implementing DevSecOps practices are embedding security into development workflows rather than treating it as a separate activity. This approach catches vulnerabilities earlier in the development cycle when they're cheaper to fix, while reducing friction for development teams.

THE CALL TO ACTION

The transformation from police officer to urban planner thinking requires leadership that can see beyond immediate threats to long-term system design. It requires courage to question fundamental assumptions about how security should work. Most importantly, it requires collaboration between security professionals, business leaders and end users to design systems that work for everyone.

For CISOs and security leaders, this means expanding our toolkit beyond traditional security tools to include design thinking, systems analysis, and user experience research. It means measuring success not just in terms of incidents prevented, but in terms of business value enabled and user experience improved.

For business leaders, it means viewing cyber security investment as infrastructure investment – something that enables competitive advantage rather than simply preventing loss. It means supporting security approaches that may be less visible but more effective than traditional perimeter-focused strategies.

For policymakers, it means creating regulatory frameworks that incentivise innovative security approaches, while maintaining appropriate protection standards. It means thinking about cyber security as essential infrastructure that requires collective investment and shared responsibility.

The choice between the police officer and urban planner models isn't just about security effectiveness – it's about the kind of digital society we want to create. We can continue building digital environments that feel like police states, where every interaction is monitored and every user is a potential threat; or we can build digital cities that enable human flourishing while maintaining safety and security through elegant design.

The urban planner's approach won't eliminate all cyberthreats, just as well-designed cities don't eliminate all crime. But it can create digital environments where security enhances rather than impedes human potential, where resilience is built into the foundation rather than added as an afterthought, and where the benefits of our connected world can be enjoyed by everyone.

The question isn't whether we can afford to make this transition. In an increasingly connected world, the question is whether we can afford not to. •

Maryam Shoraka is Head of OT Cybersecurity Operations and a seasoned security executive with extensive experience building world-class 24/7 security operations centres and developing cyber resilience strategies. Having previously served as Acting CISO and Head of Cybersecurity Operations, she specialises in helping organisations to rapidly recover from high-impact cyber incidents.

Resources and references

Government and industry reports:

Australian Cyber Security Centre. (2024). Annual Cyber Threat Report 2024. Canberra: ACSC.

Australian Government Department of Home Affairs. (2023). Australia's Cyber Security Strategy 2023–2030. Canberra: Commonwealth of Australia.

Australian Bureau of Statistics. (2023). Digital Inclusion Index 2023. Canberra: ABS.

Academic research:

Michael, K. (2023). 'Metrics That Matter: Measuring Cybersecurity Effectiveness in Digital Transformation.' University of Wollongong Cyber Security Research Centre.

Privacy Commissioner Australia. (2023). Notifiable Data Breaches Report: January to June 2023. Sydney: Office of the Australian Information Commissioner.

Industry analysis:

Microsoft Security. (2024). Digital Defense Report 2024. Redmond: Microsoft Corporation.

Deloitte Australia. (2024). Future of Cyber Survey 2024: Australian Perspectives. Sydney: Deloitte Access Economics.

Urban planning and design references:

Gehl, J. (2010). Cities for People. Washington: Island Press.

Alexander, C. (1977). A Pattern Language: Towns, Buildings, Construction. New York: Oxford University Press.

Melbourne City Council. (2022). Laneways and Urban Design: 25 Years of Transformation. Melbourne: MCC Urban Planning Division.

Technology and security framework resources:

Google Cloud Security. (2023). BeyondCorp: A New Approach to Enterprise Security. Mountain View: Google LLC.

NIST Cybersecurity Framework. (2023). Framework for Improving Critical Infrastructure Cybersecurity Version 2.0. Gaithersburg: National Institute of Standards and Technology.

Australian Digital Transformation Agency. (2024). Digital Service Standard. Canberra: DTA.

Professional organisations:

Australian Information Security Association (AISA): www.aisa.org.au

Australian Cyber Security Centre: www.cyber.gov.au

Financial Services Information Sharing and Analysis Centre Australia: www.fs-isac.org.au

Building an AI future that is Secure by Design

BY JULIAN FAY, CHIEF TECHNOLOGY OFFICER, SENETAS

ARTIFICIAL INTELLIGENCE (AI) is reshaping the world of work, and with it comes an infrastructure boom. Governments and enterprises are investing billions in the networks, data centres and the energy generation that will power AI systems – systems that look set to become new critical infrastructure for economies, defence and national security.

These mass-investment moments come rarely. It is our job as cyber security professionals to ensure that security is not an afterthought to cost and speed – as it has been in the past. The concept of 'Secure by Design' has been gaining momentum, because it aligns with what governments and large enterprises want to see happen this time around. Defined by the Australian Cyber Security Centre, Secure by Design is the practice of building security into technology from the very beginning. It means ensuring only authorised personnel have control over how data is managed, which technologies are used, and who operates them.

Those three lenses are going to become part of our day-to-day lives. The value of AI systems rests on the data they process and the decisions they influence. If those systems are compromised, the consequences can ripple across entire sectors. At the same time, AI development is shaped by geopolitics. Nations have different approaches to censorship, intellectual property and technology control. This is fuelling demand for sovereign solutions in defence, cyber security and other areas where trust is paramount.

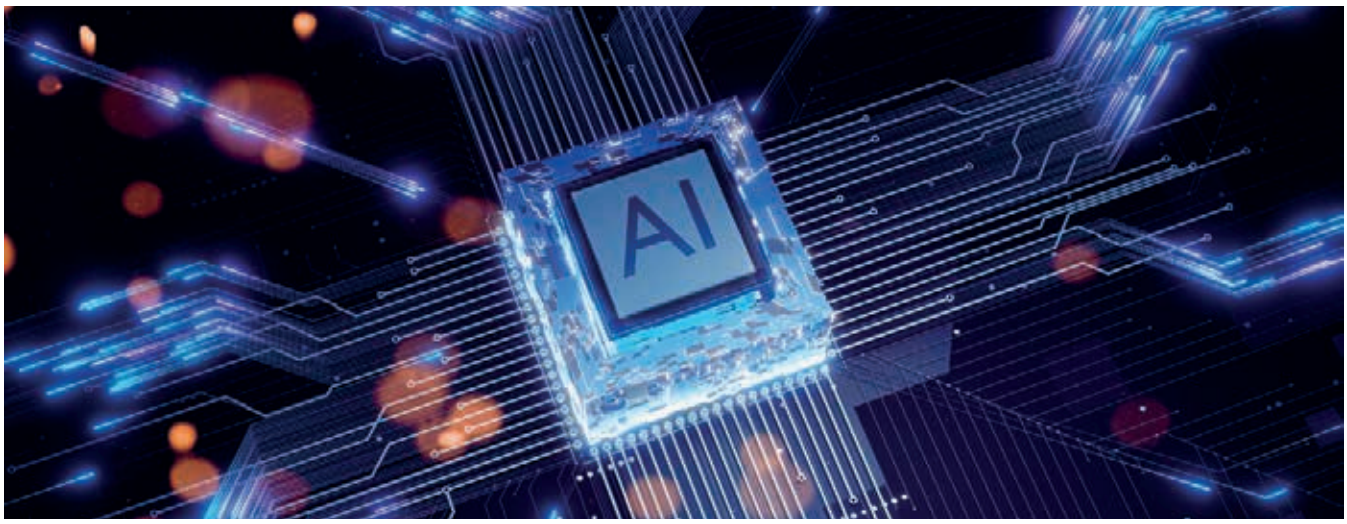
Secure by Design moves the debate beyond the question of where data is stored to ensuring complete autonomy over how technology is built, where it is operated, and how it is secured. Each nation will have its own preferences – some will be more comfortable with certain aspects of AI being outsourced than others.

Secure by Design is not a single technology, but rather a philosophy – one that spans identity management, secure software development practices, supply chain assurance and strong cryptography. Among these pillars, high-assurance encryption plays a critical role. It ensures that sensitive data remains protected in motion, regardless of the network path, and that organisations retain sole control over their keys and security policies. Certifications such as Common Criteria and Federal Information Processing Standards provide independent assurance that these systems are free from hidden vulnerabilities and perform exactly as claimed.

In critical infrastructure, where failure can have sector-wide consequences, encryption must also be built to withstand the next wave of threats – including those from quantum computing. Standards bodies and governments are already calling for quantum-safe algorithms to be deployed now, recognising that migration takes time and the stakes are too high to wait for a breakthrough to arrive.

Julian Fay

At Senetas, we work with governments and enterprises to help turn these principles into practice – designing sovereign, resilient systems that are secure from the outset and stay secure as technology evolves. The AI infrastructure boom is a once-in-a-generation opportunity to get this right. We've grown used to a world where our personal details are leaked routinely. Let's not let that happen to our prompts. Let's ensure our AI is Secure by Design. ●



SENETAS

Secure the entire journey

FROM YOUR NETWORK TO THE CLOUD

Your data is always moving—between firewalls, through clouds, and over networks you don't own. We call this the 'data in motion' problem.

Your data is also vulnerable when it's still, residing on servers, in the cloud, and in shared files—the 'data at rest' problem.

Senetas provides the complete solution. We secure your data in motion with our high-speed encryptors and protect your data at rest with our SureDrop secure file-sharing solution.

Trusted globally by governments, defence, financial services and critical infrastructure, we deliver uncompromising security for your data's entire journey.

senetas.com

FACTORED AUTHENTICATION AND PASSWORDLESS SOLUTIONS

BY RANDALL C HUGHSON, DIRECTOR, SPECTRAL CYBER SECURITY AND STRATEGIQ AI

Defence and critical infrastructure–grade considerations for multi-factor authentication and identity management.

The world of passwords, passphrases, factored authentication and identity verification has certainly come a long way over the past decade. Remember the days when you could log into banking or a web dashboard without having to enter a secondary code or confirm via your authenticator app? Those days are fast moving behind us. But don't celebrate just yet – there remains plenty of critical data out there barely protected by good passphrases, let alone multi-factor authentication (MFA) or other basic security techniques.

Access and identity management continues to be a global critical risk, demonstrated by the daily success that cybercriminals enjoy when allowed through the front door by an effective phishing or identity compromise scam. Then there are growing artificial intelligence–driven compromises led by increasingly desperate people across a turbulent geopolitical landscape.

As with most technology, seamless uptake by end users – humans, mostly (and machine or service accounts) – follows an evolutionary path and takes time. Solutions need to be not only technically and economically viable, but also centred on the people aspect of the organisation – otherwise, issues can arise with user understanding, adoption resistance and, ultimately, organisational security posture.

All this makes passwordless solutions and device-based factored authentication so much more compelling.

Consider that passwordless MFA offers a good starting point for general user access and identity security. A user can then be cross-verified via a combination (multiple factors) of something they have (a hardware security module (HSM), like a keypad token), something they know (a pin code for the HSM), and something they are (biometrics or similar).

Let's see where we can go with this.

Imagine you're a new staff member at industry subcontractor Widget Defence. Naturally, Widget Defence treats security extremely seriously, as they have sensitive intellectual property, highly vetted staff and significant market contracts. They adopt a Zero Trust methodology.

The organisation would like to vet your background and identity using a third party, so that your identity is independently confirmed as authentic and cannot be repudiated – two key pillars of cyber security methodology. Once they are satisfied with this, only then will Widget Defence be issued with a digital account (granting you access), and an HSM that meets the above MFA criteria (the identity management piece).

Now, don't diminish the importance of good human identity verification – you'd be amazed by how many large organisations do surprisingly little to verify user identity and background within their own teams, let alone via a third party. Doing this can add massive strength to the identity solution at hand.

Let's do even better! Let's imagine that the HSM and MFA solution is part of an infrastructure ecosystem that integrates alongside Widget Defence to log, monitor and validate MFA, and explicit data access in real time. The identity – user or account – can be automatically cordoned if compromised at full identity level, perhaps in tandem with actions we may see systemically with a managed detection and response tool.

Now we're well down the path of modelling what might constitute a defence-grade approach, and this is exactly what we're now seeing several critical infrastructure sectors seriously explore further, particularly given current geopolitical considerations where criminal data activity and espionage are commonplace.

This is also what we see emerging with everyday folks longer term. Consider the future benefits, for example, as we move toward Digital ID.

Of course, there's far more detail to the solution approach than what can be outlined here, but there are a few additional points that you may find beneficial if considering what good MFA can be, characteristics of an HSM, and the sort of solution your organisation can start to explore:

- MFA should be phishing-resistant. That's a term you're going to hear a lot more about as our identity-verification methods – and their application – get more sophisticated and widespread.
- Any solution should aim to simplify end user experience. We all can have midnight brain fade and enter a code or pin where we shouldn't. You want a tool and ecosystem in place that caters to that potential exposure.
- Dedicated MFA HSM's will generally be far more secure than smartphones and apps.
- You want to minimise the potential attack surfaces, so an MFA solution and HSM should streamline identity and access control across multiple services within the organisation, not just, say, Microsoft 365.
- An HSM should be easy for someone to carry without being an encumbrance. For instance, easily stored in a smartphone case or on a lanyard.
- Technical certifications will show you the standard of the technology – Common Criteria (for defence grade), EMV and PCI-PTS should be observed.
- Though not unique, make sure an MFA solution (and HSM) observe protocols such as Microsoft Entra AD integration standards, FIDO, or OAuth (particularly for protecting identities on third-party web-based services).

Finally, there's one crucial and often overlooked component required alongside any HSM-based MFA solution, no matter the organisation, and it applies to cyber security generally: cyber training and awareness – delivered in a way that real humans understand and enjoy!

As you explore and embark on strengthening your organisation's identity through phishing-resistant, certified MFA and highly secure, easy-to-use HSM solutions, never forget the need to bring your team along for the journey. It's taken great time and effort to date to get society used to the more basic security techniques like good passphrases and authenticator apps, and we all know how challenging it can be sometimes for those not using tech every day. Let's collectively use that experience to actively keep our people – our society – as secure as possible given where we're heading on the privacy front. Our future society will almost certainly appreciate it! ●

Randall C Hughson is a cyber security and infrastructure consultant, director, public speaker, and presenter with more than 25 years' experience in private enterprise and government. He specialises in general security techniques, infrastructure planning and analysis, identity management and cyber-first response, and is particularly adept at engaging company leaders, boards, and owners on a cyber journey. A regular speaker at the Australian Information Security Association's CyberCon, and at schools and business training forums, he brings an engaging and compelling approach, making the information relevant and accessible to all. On the side, he's an experienced performing musician (saxophone and piano), and a martial artist, and has a keen interest in global sustainability and space exploration.

Cyber frontlines: Australia's defence imperative in an era of rising conflict

BY JACQUI KERNOT, VICE-PRESIDENT CYBERSECURITY, THALES

THE BATTLEFIELD IS no longer defined by geography alone. Cyber capabilities, autonomous systems and information warfare are reshaping the strategic landscape. And, like many of our allies, Australia is already moving to meet these emerging challenges.

Maintaining global and regional stability demands not only traditional firepower, but also a huge shift in how we defend our digital infrastructure and safeguard national sovereignty in the information age. This more sophisticated, tech-driven cyber offence must be matched by defence-grade cyber protection.

The focus should be on capability – ensuring that Australia can operate effectively in a security environment defined as much by cyber disruption and economic coercion as by conventional force.

As the only defence-grade cyber security company in Australia, our purpose at Thales Australia is to deliver national security and resilience while protecting the nation and our partners – making them all safer.

As the steward of Australia's defence industrial base, Thales Australia has a proven track record in delivering sovereign capability. Our Australian-made sensors serve aboard Royal Australian Navy ships, submarines and vehicles. Meanwhile, the Bushmaster Protected Mobility Vehicle has been a critical asset for the Australian Defence Force for decades – designed and manufactured in Bendigo. This is what sovereign capability looks like: an Australian-designed and -built system, deployed globally, and refined over decades of real-world operations. As the threats evolve, our industry must also pivot.

Today, devastating attacks may not come from missiles, but from malware. Critical infrastructure – ports, power stations, airports, health systems and financial networks – is increasingly in the crosshairs of nation-state actors. Our very identities in a digital age can be vulnerable to attacks.

Cyber resilience is now a cornerstone of national security. Just as defence platforms like the Bushmaster protect our troops, we are providing digital capabilities that protect our systems, services, institutions, and identities.

Australia must invest in both steel and software – warfighting platforms and cyber defences. Every attack on our infrastructure, every attempted intrusion into our networks, is a reminder that our adversaries are probing for weakness.

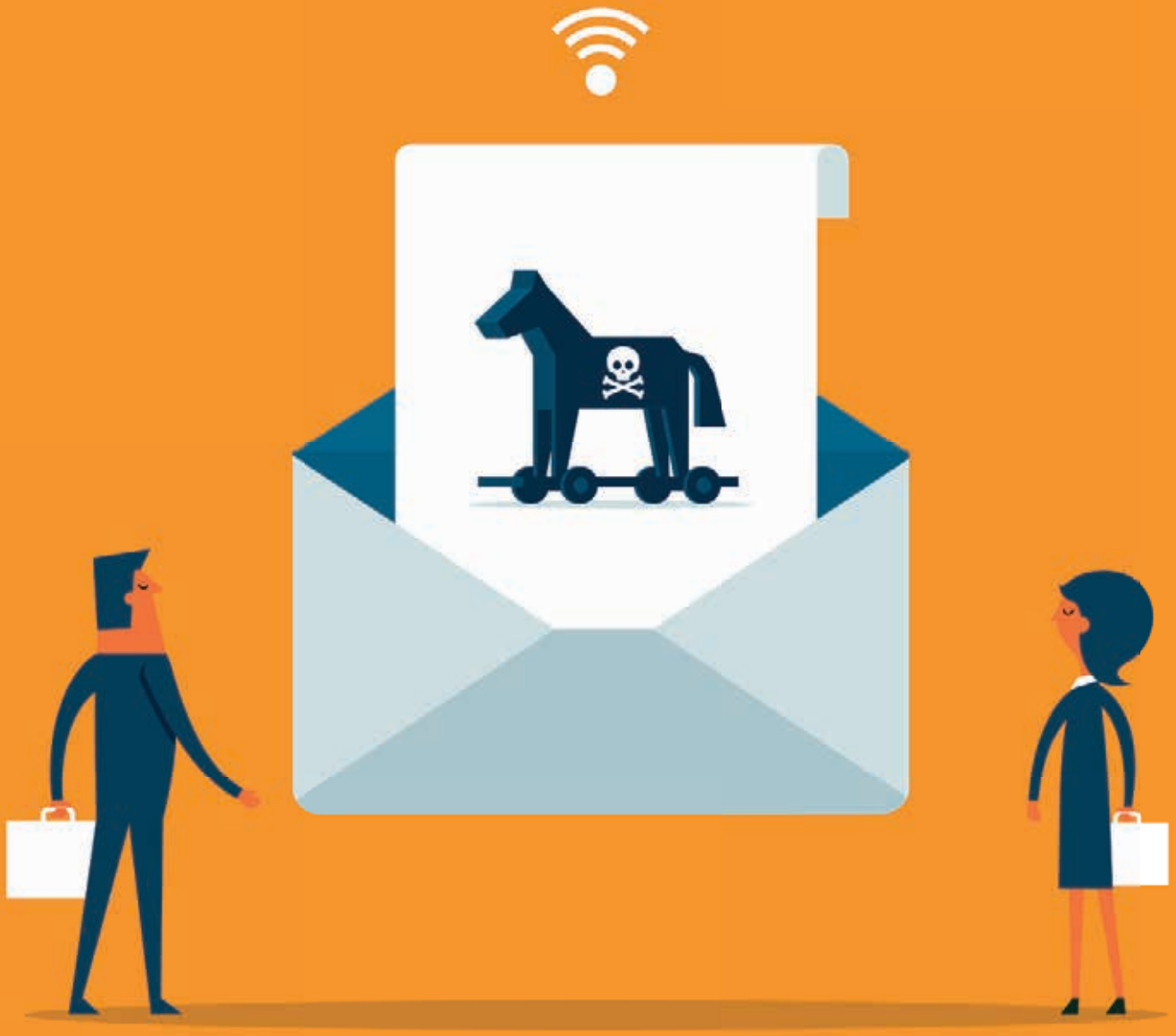
Jacqui Kernot

Thales Australia is responding to this national security imperative by expanding our contribution to cyber resilience. In 2023, we established a new cyber security services division to support the protection of Australia's most critical systems – from defence platforms to energy networks, transport hubs and financial infrastructure.

We blend the innovative tech company mindset with the security-focused power of Australia's sovereign defence prime – allowing us to provide unmatched security for what matters most: applications, data, identities and critical infrastructure. Thales is already directly protecting the identities and data of many Australians through our digital ID solutions that incorporate privacy-by-design.

Because the next conflict may start with a signal – not a shot – it is our mission to work with government to build a resilient, sovereign capability base.

As the steward of Australia's defence force manufacturing capabilities, Thales Australia has stood alongside the Australian Defence Force since 1912. We have extended that commitment to the cyber domain – helping to safeguard Australia's digital foundations with the same focus, reliability and resolve. ●



THE ROLE OF EMAIL SECURITY IN AN AI WORLD

BY KYLE WATERS

Email security is the practice of protecting email accounts and communications from unauthorised access, attacks, loss and compromise. To put it another way, it is the frontline defence for almost every company that operates online or has an online presence in some capacity.

Between 91–96 per cent of all direct cyber attacks begin with a phishing email, and 32 per cent of all successful breaches involve the use of phishing techniques either prior to or during the breach event.

WHY IS EMAIL SECURITY SO IMPORTANT IN AN AI WORLD?

Due to the evolving nature of technology – specifically artificial intelligence (AI) – traditional cyber security is also having to evolve. As email security is often the tip of the shield, it is encountering the earliest waves of newer attacks, as well as more refined versions of traditional ones.

WHAT ARE THE KEY PILLARS OF EMAIL SECURITY?

There are three key pillars of email security. These form the foundation of a good email security platform: encryption, filtering, and training/education.

- **Encryption:** Email encryption is the first line of defence when it comes to protecting any message that needs to be sent securely. Even if a message is intercepted, it cannot be easily accessed or read. Anything sent in the clear is not secure – it's public.
- **Filtering:** Email filters are designed to automatically sort out spam, malware and viruses by scanning the body/content, attachments, and links for known or suspected malicious software and phishing attempts before they reach the recipient. Email filtering is best compared to having a digital security guard, checking details to ensure only authorised messages get through.
- **Training/education:** Training and awareness programs teach users to identify and properly report threats to IT. Through training and education, people shift from being the last line of defence to the first, or at least another strong layer of security. The more we teach and learn, the more we put into practice.

HOW ARE CYBERCRIMINALS ALREADY USING AI TO GET AROUND TRADITIONAL EMAIL SECURITY TOOLS?

Cybercriminals have shown rapid adoption of AI tools, including generative AI (GenAI) and large language models. The majority of organisations report that they have already encountered email attacks enhanced by AI.

For example, AI algorithms are used to automate aspects of phishing campaigns, including mass email generation, domain spoofing and content personalisation. By analysing and compiling vast amounts of data, AI-powered tools can craft convincing phishing emails tailored to individual recipients. This increases the likelihood of success, decreases the time needed to execute phishing and spear-phishing campaigns, and allows these attacks to be conducted at greater speed and frequency.


Kyle Waters

Data collection teams, cybercrime groups, nation-state threat actors and independent attackers are using AI tools to collect and analyse private data in greater detail than what was previously possible. This may be done either for their own attacks or simply to sell the reconnaissance to others without tipping off the target during the information-gathering phase.

Evading security measures is another malicious use of AI. For example, AI-powered malware can be designed to adapt its behaviour to evade detection by traditional cyber security measures, including those developed in-house by the target. This makes it more challenging to detect and neutralise, even when using third-party or vendor-built tools and systems.

Data-poisoning attacks are also a concern. Attackers can manipulate previously acquired data used to train AI applications. For example, an attacker could subtly modify an image to fool an image recognition system into misclassifying objects, or embed malware into the data layers of an image.

HOW TO SPOT AND TRACK AI-AUGMENTED ATTACKS

- **AI-powered content analysis:** Vendors are increasingly incorporating GenAI into their analytics platforms. Generic and third-party tools can also be used for more manual analysis.
- **Consistency versus randomness:** AI-generated content tends to be overly consistent and uniform in sentence length and structure, whereas human-generated content is more varied.
- **Repetitive words and phrases:** Because AI vocabulary is constrained by its language models, content may include unnecessary repetition where humans would use more natural alternatives.
- **Incorrect grammar and punctuation:** AI-generated content sometimes suffers from awkward grammar or misplaced punctuation, making it harder to read.
- **Incoherence:** AI can struggle with interpretive analysis, context, or maintaining a consistent, coherent argument.
- **Lack of sourcing:** AI-generated text often lacks credible or verifiable sources, especially when referencing online content.
- **Devoid of personality (the 'human touch'):** While personality isn't always necessary – such as in legal, medical or corporate emails – other types of

communication are expected to be more colourful or conversational. The absence of this can be a giveaway.
- **Doesn't pass the smell test:** Ultimately, human instinct and critical reading remain invaluable in spotting AI-generated content.

AWARENESS AND CONTINUOUS ASSESSMENT

Cyber awareness and education are among the best methods of detection and protection. The more people are aware, the more likely they are to practice safe behaviours. Through practice, these behaviours become instinctive, increasing the likelihood that individuals contribute to your defence rather than compromise it.

Regular assessments of your email security platform also help locate blind spots that you or your vendor can work to close. More importantly, assessments determine whether you should stick with your current platform or consider an upgrade. These reviews reveal whether your vendor is the best fit for your company – and if not, it may be time to look elsewhere. Loyalty is good, but security is better.

SIMPLE EMAIL SECURITY STRATEGIES TO STAY AHEAD OF THREAT ACTORS

- Update and maintain email security policies, definitions and exceptions in your platform. Gone are the days of 'set and forget'. Neglecting updates allows attackers to find ways around defences, and outdated systems may block too many legitimate messages while still letting malicious ones through.
- Conduct regular penetration testing of the email security environment. Probe your own systems to find weaknesses before someone else does.
- Use multiple email security layers. Not all platforms are created equal, and a layered approach increases protection.
- Run both scheduled and ad hoc phishing campaigns. People can become complacent with routine tests, so mixing in unexpected campaigns helps to keep them alert.
- Cyber awareness and education cannot be stressed enough. It is critical for everyone.

In summary:

- Email security is the frontline of defence: it protects sensitive information and helps to prevent data breaches.
- Cybercriminals are already using or developing AI-augmented attacks. Incorporating GenAI into email security platforms will help, but preparation is essential.
- The key question isn't 'How do we defend against AI?' or 'How do we get AI to defend us?' Rather, it's: 'How do we combine AI with what we already know to improve our defences?'
- A healthy level of suspicion is useful – if a message doesn't feel right, report it.
- Education around email security is paramount. ●

Kyle Waters is a self-described 'polymath' who, in addition to various retail, hospitality, and volunteer roles, has worked in technical and support roles for more than 20 years. In that time, he has developed an extensive range of knowledge and training across multiple disciplines. His qualifications include a Certificate IV in Cybersecurity, ITIL V3 & V4, CCNE Levels 1 & 2, Certificate III in Training & Mentoring, and Certificate IV in Sound & Lighting, most of which he completed while working full time in unrelated fields.

RAPID7

PROUD SPONSORS OF CYBERCON MELBOURNE

TAKE COMMAND

OF YOUR ATTACK SURFACE FROM ENDPOINT TO CLOUD

Visit us at **BOOTH 85** TO CHECK OUT OUR LIVE PATCH BAR

Ask for a demo

Ask for a live demo and witness the power of Rapid7 in action. Our experts can showcase the following:

MDR with Unlimited Incident Response

Gain 24/7 XDR monitoring, remediation and DFIR from SOC experts

Exposure Management

Get continuous assessment and validation of your attack surface

Next-Gen SIEM

Pinpoint threats wherever they start with cloud-first detection and response

Cloud Security

Secure multi-cloud environments with complete visibility

Vulnerability Management

Understand risks across hybrid environments

Threat Intelligence

Discover and remediate external threats

The four pillars of human risk management

WHEN IT COMES to cyber security, organisations face an ever-present and often underestimated threat: human risk. Despite significant advancements in defences, human error remains the leading cause of data breaches and security incidents. Multiple industry studies and research reports consistently show that between 70 and 90 per cent of data breaches involve some form of human-related cause – whether through social engineering, mistakes or misuse. Moreover, a recent study revealed that 74 per cent of CISOs now consider human error their top cyber security risk. This stark reality has led to the emergence of human risk management (HRM) as a critical component of comprehensive cyber security strategies.

HRM aims to identify, quantify and mitigate risks associated with human behaviour in a cyber security context. And while the term HRM may be relatively new, the concept itself represents years of evolution in understanding how to effectively address human-related security risks. This human-centric philosophy stands in sharp contrast to traditional security awareness approaches that often focused on simply making employees aware of risks while potentially blaming them for mistakes.

HRM represents a paradigm shift from traditional security awareness training approaches. While conventional methods focus primarily on knowledge transfer, HRM adopts a more holistic, data-driven approach to understanding, measuring and mitigating risks associated with human behaviour in digital environments. HRM platforms leverage artificial intelligence (AI)–driven analytics and adaptive security architectures to create a comprehensive and dynamic defence that evolves with the threat landscape.

PILLAR ONE: RISK IDENTIFICATION AND ASSESSMENT

Before you can manage human risk, you need to understand it. The first step is building visibility into employee behaviours and vulnerabilities. Modern HRM platforms use AI-driven analytics to move beyond superficial metrics like training completion, helping security teams to zero in on the individuals, groups or roles most exposed to specific threats. This foundational visibility is the starting point for everything else.

PILLAR TWO: PERSONALISED EDUCATION AND ENABLEMENT

Generic, one-size-fits-all training doesn't cut it anymore. The second pillar of HRM focuses on personalisation – turning security awareness into an ongoing, engaging experience that fits each employee's role, learning style and risk profile. The goal isn't just to make employees 'aware' of threats, but to make secure behaviour intuitive and easy. AI and machine learning help to deliver adaptive training that evolves with each user, reinforcing positive habits where they're needed most.

PILLAR THREE: TECHNOLOGY INTEGRATION AND AUTOMATION

The third pillar brings everything together. Effective HRM platforms integrate with the rest of your security ecosystem – SIEMs, endpoint detection, email security and more – to correlate human risk data with technical controls. Automation plays a big role, streamlining time-consuming tasks, such as campaign creation, reporting and even responses to user-reported phishing. This doesn't just improve security outcomes; it frees your team to focus on higher-value work.

PILLAR FOUR: CONTINUOUS MONITORING AND IMPROVEMENT

Finally, HRM is not a one-and-done project. Human risk changes constantly – as employees change roles, threats evolve, and attackers adopt new techniques. The fourth pillar emphasises ongoing measurement, adaptive controls and a feedback loop that keeps your program sharp. The most successful organisations treat HRM as a living system – always learning, always improving. ●

knowbe4

Reduce Risk Where It Starts: Human Decisions

Human Risk Management +

+ 15+ years of threat & user intelligence data

+ Industry-leading cloud email security

+ AI-driven security awareness training

Visit KnowBe4.com to Learn More

AUSTRALIA IS FIXING A BROKEN HEALTH INTELLIGENCE MARKET

BY DR HUON CURTIS, CI-ISAC AUSTRALIA

Your healthcare system, power grid, or local council network is one successful phishing email away from making headlines. And the team responsible for defending it has 40 high-priority projects, three people to do them, and a chorus of vendors telling it that artificial intelligence will solve everything. This disconnect between the solutions being marketed and the reality of keeping critical infrastructure secure isn't just about technology – it's about having the right intelligence at the right time, in a format you can actually act on when your team is already stretched beyond capacity.

Answering this need for smarter, more focused intelligence is at the heart of a transformation in Australian cyber threat intelligence (CTI). In line with the Australian Information Security Association conference theme, 'Transform to Evolve', the answer lies in a new, national-scale approach, and it's being tested right now in one of our most critical sectors: health care.

THE MARKET FAILURE UNDERMINING OUR DEFENCES

A senior health cyber professional recently told us, 'I receive hundreds of alerts, but I've stopped checking them. I don't have time to figure out which are relevant.'

This isn't a personal failing; it's a systemic one. The professional is drowning in noise because we have fundamentally confused alerts with intelligence. This 'signal versus noise' challenge is the direct result of a broken intelligence market that creates weak spots that attackers easily exploit.

The market offers a false choice. On one hand, commercial intelligence carries a prohibitive price tag, putting it out of reach for many that form our infrastructure's backbone. On the other, public domain intelligence, while valuable, is often too generic to be actionable, simply adding to the noise.

Worse, both sources are often disconnected from the Australian context – our approved technologies and regulatory conditions. This forces security teams to waste precious time translating global threats into local risk. The result is a fragmented defensive landscape where the organisations most in need of timely, contextual intelligence are the least able to access it. There is a substantive difference between an alert that advises to 'patch your system', and a step-by-step advisory that clearly steps out how to close a vulnerability.

THE BOARDROOM IS NOW ON THE HOOK

The average cost of a data breach in Australia is now nearly $4 million, according to IBM's recent Cost of Data Breach 2025 report; but, for a regional hospital on tight margins, even a 'small' breach can mean cutting essential patient services. A new era of executive accountability for cyber risk has arrived, with legal pressure mounting from multiple fronts. Regulators like the Australian Securities and Investments Commission and the Office of the Australian Information Commissioner are pursuing boards and directors directly, as seen in the cases against RI Advice Group and Optus. Consumers are taking action themselves – a class action lawsuit against Genea Fertility recently commenced.

This intense pressure on leadership creates a vicious cycle. To meet their new obligations, boards

require foundational security services like risk audits, penetration tests and compliance assessments. Yet, we've heard directly from health operators that the quoted prices for these essential first steps are simply unaffordable. They are trapped: legally accountable for a standard of security they are economically blocked from achieving, leaving them exposed and unable to even begin the journey towards resilience.

A THIRD WAY: NATIONAL-SCALE, NOT-FOR-PROFIT INTELLIGENCE

To close this gap, the Australian Government has funded a bold innovation through its 2023–2030 Cyber Strategy: the Health Cyber Sharing Network (HCSN), delivered by the not-for-profit Critical Infrastructure–Information Sharing and Analysis Centre (CI-ISAC). This initiative builds a whole-of-nation capability tailored specifically to Australia's unique threat landscape and regulatory environment.

The innovation is straightforward: a member-owned, not-for-profit ecosystem to curate and share CTI. Instead of just distributing raw data, CI-ISAC's analysts – in collaboration with members – filter, contextualise and prioritise threats. We test malware in our own sandbox and pull apart vulnerabilities.

The result is practical advisories delivered via our portal that tell you what's broken, how it affects you, and exactly what to do about it. They are designed to be immediately actionable for everyone – from a junior analyst in a regional hospital, to a seasoned threat hunter at a Tier-1 bank.

We're also tackling one of the most neglected yet critical areas of cyber risk: the vulnerabilities buried deep inside operational technology. Much of our nation's infrastructure runs on 'black box' devices – from medical instruments in hospitals, to the firmware in network switches – where the underlying software is a mystery to the owner. We proactively identify systemic risks in the digital supply chain, giving our members

a critical head start on protecting systems that are difficult to secure.

Because CI-ISAC is a not-for-profit, our mission isn't shareholder return; it's securing Australian infrastructure. This allows us to make high-quality intelligence and other resilience-building resources accessible to organisations of all sizes, democratising security and helping members to begin the journey to resilience.

The response has proven that the demand for this new model was there all along. In just six months since launching in February 2025, we've brought together a diverse cohort of members spanning the private and public sectors, and state governments. This groundswell of support confirms a significant pent-up demand for a better way to build national cyber resilience. Today, our network includes organisations across the entire health value chain – from insurance, hospitals, philanthropies and biopharmaceuticals, to critical pharmacy and supply chain providers – that collectively serve more than 12 million Australians.

COLLECTIVE DEFENCE IN ACTION

The power of this model lies in what we call collective defence: when one member shares a threat observation, CI-ISAC turns this into actionable intelligence and everyone benefits. The network effect amplifies our defensive capabilities as insights flow between organisations that are defending against the same attackers.

This isn't just theory. We see it working every day:

- **The 'ClickFix' campaign:** A healthcare member shared details of a novel incident. Our team analysed the malware, identified its techniques, and discovered it was a 'ClickFix' campaign designed to bypass conventional security, leaving few traces. Our analysis uncovered 70 indicators of compromise (IoCs) – a huge leap from the three IoCs published elsewhere. An actionable advisory went out to all members, protecting them from a threat they otherwise wouldn't have seen coming.
- **Social engineering techniques:** A member discovered a sophisticated social engineering attack on their call centre in mid 2023, which was attributed to the Scattered Spider group, with further reported impacts against four critical infrastructure sectors. We issued an advisory with actionable guidance on how to detect specific vishing techniques, helping members to educate service desk staff and harden against the human attack vector.

In both cases, a key insight from one member helped to protect the entire community. This is the future: moving from isolated defences to a collaborative, national immune system, from reactive response and recovery to effective preparedness and pre-emptive mitigation.

BUILDING CAPABILITY, NOT JUST SENDING ALERTS

The HCSN's innovation goes beyond just sharing CTI; we focus on making it actionable. We recognise that many organisations struggle to consume CTI effectively because they lack fundamental visibility. As one member put it, 'You can't share anything meaningful if you don't have visibility.'

This visibility isn't just about having the right automated tooling, like a security information and event management solution. True visibility is strategic: it requires executive-level engagement to identify an organisation's most valuable data and the deliberate selection of tools to protect it.

Intelligence is only valuable when paired with the capacity to act, and our model is designed to build that very capability. In time, our practical resilience resources, attack surface monitoring and cyber exercising will further empower our members to turn intelligence into an effective, active defence.

THE OLD PLAYBOOK IS BROKEN

For years, 'information sharing' has been a cyber security buzzword that promised much but delivered little. Past efforts often failed because they were built for a world that no longer exists – a world with clear lines between corporate risk and national security.

That world is gone. Today's ransomware groups function like multinational corporations, and state-sponsored attackers operate with the ruthless sophistication of a tech startup. They share tactics, infrastructure and intelligence.

This new reality is forcing a global rethink. The United States and the European Union are already mandating closer public–private collaboration, and Australia cannot afford to be left behind with a fragmented approach. This isn't about sharing information for its own sake; it's about building an operational defence capability that matches the scale and coordination of our modern adversaries.

A MODEL FOR NATIONAL RESILIENCE

While the initial HCSN pilot focuses on health care – a sector grappling with everything from legacy medical devices, to patient safety – the model is designed to scale. The lessons learnt and the infrastructure built through the HCSN provide a template for closing intelligence gaps across all 11 of Australia's critical infrastructure sectors.

The challenge ahead is to evolve beyond the reactive, fragmented security models of the past. Incremental improvements won't be enough – we need a transformation in how we collaborate, share information and build collective resilience. By creating a nationally focused, member-driven institution, Australia is pioneering a new way forward – demonstrating how we can transform to evolve, together. ●

The importance of minimum viable recovery

RECOVERING EVERYTHING AFTER a cyber incident isn't just challenging – it's often impossible to do quickly. This is where the concept of minimum viable recovery (MVR) becomes essential: identifying and prioritising the critical subset of business functions absolutely necessary to maintain operations during a crisis.

When organisations face cyber attacks, they often discover a disconnect between their technical recovery capabilities and actual business needs. According to the 2025 State of Data Readiness Report commissioned by Commvault via Tech Research Asia, the gap between business leaders' recovery expectations and the on-the-ground reality for IT teams remains a major issue for those surveyed. Eighty per cent of business leaders expect to recover from a cyber security incident within five days. The stark reality, however, is that it takes an average of four weeks to restore a minimal level of business operation. Furthermore, 70 per cent of organisations across Australia and New Zealand have received a ransomware demand; and of those, 20 per cent admitted to paying it. Interestingly, of the companies with a stated 'no payment' policy, 15 per cent still ended up paying the ransom when faced with an actual attack. This 'recovery gap' exists largely because recovery planning is typically technology-led rather than business-driven.

Traditional recovery approaches often attempt to recover everything, which can lead to:

- extended downtime for critical systems while less important systems are restored
- resource allocation that doesn't align with business priorities
- recovery timelines that far exceed business tolerance for disruption
- technical teams making business-impact decisions without proper context.

In order to implement an MVR approach, the first step is to identify the subset of business functions that are truly essential: critical revenue operations, customer-facing services, regulatory requirements, supply chain operations and employee productivity. Organisations that take a business-led MVR approach can achieve the same level of risk mitigation as those pursuing comprehensive recovery – but faster, and at lower cost. The key is proactive business engagement at a strategic level before an incident occurs.

MVR represents a fundamental shift in how organisations approach cyber resilience. The strategy for recovery prioritisation should be business-led, not technology-driven, and requires cross-functional collaboration before an incident occurs. Next, alignment on recovery priorities between technical and business functions is critical – knowing what matters most will mean resources are working together in the midst of a crisis. Lastly, regular testing and validation from a business perspective is essential.

By focusing on what truly matters to your business, you can achieve more effective resilience with fewer resources, lower cost, and greater confidence in your ability to weather cyber disruptions. ●

Gen Z's apathetic approach to online privacy hurts our cyber security

BY AUDREY FITZGERALD

As a gen Z student of computer science and cyber security, I have a unique perspective of my generation's blasé attitude to online privacy and the a growing security risk it poses.


Audrey Fitzgerald

If this blasé attitude to cyber security was simply due to a lack of education on the risks to online privacy, then maybe universities and TAFEs could address that. It's not. Generation Z (gen Z) grew up in the internet era; we're tech-literate because we've been immersed in tech. Many of my classmates have never bought a postage stamp or mailed a letter in the post.

Online is our life. In the United States, 62 per cent of people aged 18–29 say they're online 'almost constantly' – a figure far higher than for older groups.[1] In the United Kingdom, young adults spent the most time online, with 18–24-year-olds spending a daily average of six hours and one minute.[2]

So, why is it that millennials (gen Ys) reported safer practices on several key behaviours than gen Z? A peer-reviewed study of 593 students at two universities compared college-aged gen Y to gen Z, and found that gen Y reported higher engagement on four of eight security behaviours, including reviewing social media privacy policies, keeping antivirus software updated, watching for unusual computer performance, and acting on malware alerts.[3]

Perhaps more worryingly is how our gen Z attitudes to giving up privacy online may be contributing to bad cyber security practices. Gen Z is the most native online generation yet. So, why is it that even though 79 per cent of gen Zs say password reuse is risky, 72 per cent still reuse passwords?[4]

I suspect a big part of this problem of my generation stems from the radical normalisation of giving up our data. It is extracted so frequently from us that we give up, and give in. We've been hypnotised into taking shortcuts, buying into convenience above all else as the norm. My generation devours dystopian sci-fi shows like *The Last of Us*, but we ourselves have become the sleepwalking zombies when it comes to the privacy of our own data.

The other problem is social norms. We may be aware of privacy risks, but my generation prioritises social connection over minimising data sharing. We are the biggest users of Signal by age group cluster among iPhone users (36.1 per cent), according to one report[5]; however, we are also busy oversharing on TikTok, Instagram and Snapchat. Gen Z spends more than twice as much time on TikTok, Instagram and Snapchat as the general population.[6] About 79 per cent of gen Z uses TikTok compared with 58 per cent of gen Y.[7]

The continuous development of technology means that we have become accustomed to convenience at every turn. We have gotten used to the luxury of convenience online, which makes it more difficult/frustrating to force ourselves to jump through extra hoops and 'waste' time declining unnecessary cookies – or money on subscribing to password managers just to keep our information 'safe'.

We in gen Z have gotten ourselves into a privacy paradox pickle. There is a disparity between our concerns for online safety and privacy, and our online behaviours, which don't protect us despite our concerns. Yes, it exists for generations that have come before us, but it seems more pronounced for gen Z. For some of us, it's because we are fatigued from the vigilance needed to stay safe online, particularly given our widespread presence online as a generation. Also, there is some latent resentment about the hypocrisy here in older generations telling us to reduce information-sharing about ourselves online. Mum and Dad pasted us all over Facebook in our childhood: that means the horse has bolted on our privacy forever.

I've often heard from peers, 'If someone wanted my information or passwords, I'm sure it's already out there.' There is this perception of 'Why bother trying to secure myself when I'm already not secure online?' And if it's 'already out there', then it's only a short leap to 'Why bother inventing unique passwords for each online account?'

For others, there is a happy and wilful giving up of data for a more personalised experience. Fifty-nine per cent of UK youth know about algorithms curating their feeds; nearly half (46 per cent) of those who know about algorithms say they're happy for apps to use collected data to decide what to show.[8]

Knowing that the algorithms on social media are harvesting our personal data is seen as worth it for the experience of having tailored content.

With more countries looking into implementing age verification for social media, we wonder if we will be forced to pay a 'privacy price' to stay connected to our peers.[9] The choice becomes either forfeit your personal data to prove your age, or feel isolated among your peers. For many it will be a no-brainer – of course you'd be happy to give up your ID information if it meant you can still be connected online to your friends.

Whether you're on team blissful ('Yay! A more personalised and socially connected experience!') or team gloomy ('What's the point? All my data is out there for the taking beyond my control') – both sides of the laxness in gen Z's online privacy are likely exacerbated by the fact that gen Z are the youth of today.

A sense of invulnerability and invincibility experienced in youth is not something specific to our generation. Research has long linked youth with a greater willingness to take risks.[10,11] 'Risky behaviour' attracts youth of every generation. Earlier generations (baby boomers, gen X and gen Y) showed this in their youth by smoking, drinking and early sexual activity. Gen Z is taking fewer of these kinds of offline risks.[12] My generation doesn't feel invested. We worry about our level of personal debt and often think we will never be able to buy our own home.[13,14] We feel less of a 'stake' in our personal data, so we care for it less. Yes, we've been told that's dangerous, but it genuinely feels like there is not much for us to lose.

Is there a way back from this non-decision oblivion when it comes to gen Z's privacy and cyber security? Maybe.

During some end user training in cyber security for healthcare workers in the Middle East, I met a healthcare worker whose biggest concern regarding her cyber security was her own children. That reverberated in my teenage mind. It made me realise that our generation's risky behaviours affect not only us, but also the people around us. While we may not have important assets to protect, we become a risk for social engineering attacks to those close to us. I don't have all the answers, but it may be a starting point for opening the conversation. •

Audrey Fitzgerald is a second-year university student studying computer science and cyber security.

End notes

1. *Pew Research Center. (31 January 2024). 'Americans' use of mobile technology and home broadband'. www.pewresearch.org/internet/2024/01/31/americans-use-of-mobile-technology-and-home-broadband/*
2. *Ofcom. (2024). Online Nation 2024 report. www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-nation/2024/online-nation-2024-report.pdf?v=386238*
3. *Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). 'A reverse digital divide: Comparing information security behaviors of generation Y and generation Z adults'.* International Journal of Cybersecurity Intelligence and Cybercrime*, 3(1), 42–55. https://doi.org/10.52306/03010420GXUV5876 https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1052&context=ijcic*
4. *Bitwarden. (2025). 'World Password Day 2025 survey: 72% of Gen Z reuse passwords'. https://bitwarden.com/resources/world-password-day/*
5. *Backlinko Team. (23 June 2025). Signal user statistics: How many people use Signal? Backlinko. https://backlinko.com/signal-stats . This was based on a study of iPhone users. Among iOS users, ages 18–24 = 36.1% (largest cohort); 35–49 = 21.7%; 50–64 = 21.7%; 25–34 = 19.8%; 65+ = 0.7%. No broader public generational breakdown located*
6. *Robertson, M. (14 October 2024). 'Gen Z spend over twice as much time on TikTok, Instagram, and Snapchat compared to the general population'. Mobile Marketing Reads. https://mobilemarketingreads.com/gen-z-spend-over-twice-as-much-time-on-tiktok-instagram-and-snapchat-compared-to-the-general-population/*
7. *PartnerCentric. (10 June 2025). 'Social media use by generation: 2025 trends & statistics'. PartnerCentric. This is a US study. https://partnercentric.com/blog/social-media-use-trends-by-generation/*
8. *Ofcom. (19 April 2024). 'Children and parents: Media use and attitudes report'. OFCOM's sample was UK children aged 8-17. www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229*
9. *Ofcom. (16 January 2025). 'Quick guide to implementing highly effective age assurance'. www.ofcom.org.uk/online-safety/illegal-and-harmful-content/age-assurance*
10. *National Research Council & Institute of Medicine. (2002). 'Adolescent risk and vulnerability: Concepts and measurement'. National Academies Press. https://nap.nationalacademies.org/catalog/10209/adolescent-risk-and-vulnerability-concepts-and-measurement*
11. *Denscombe, M., & Drucquer, N. (1999). 'Critical incidents and invulnerability to risk: Young people's experience of serious health-related incidents and their willingness to take health risks'.* Health, Risk & Society*, 1(2), 195–207*
12. *Orso, L. (29 May 2024). 'Gen Z teens are taking far fewer risks. Behavioural Insights Team'. www.bi.team/blogs/gen-z-teens-are-taking-far-fewer-risks/*
13. *Australian Securities and Investments Commission. (14 November 2023). 23-302MR 'Gen Z more concerned about finances than any generation in Australia'. https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-302mr-gen-z-more-concerned-about-finances-than-any-generation-in-australia/*
14. *Grattan Institute. (28 March 2025). 'Housing is less affordable than ever'. https://grattan.edu.au/news/housing-is-less-affordable-than-ever/*

Belkin's next leap in cyber security: the latest in SKVM and beyond

FOR MORE THAN three decades, Belkin has been a quiet giant in the hardware cyber security market. Now, as threat actors evolve from shadowy individuals to nation-state-level adversaries, the company is doubling down on secure hardware for the world's most sensitive environments.

HA-5 SERIES SECURE KVM: THE COMMAND CENTRE FOR THE CLASSIFIED ERA

The new HA-5 Series Secure KVM isn't just a switch – it's mission control for the multi-domain desktop. Built for classified networks and high-assurance workplaces, it consolidates multiple isolated systems into one secure console – all without ever letting data leak between them.

It consolidates control of multiple isolated systems into a single console, while adding support for webcams, headsets, push-to-talk audio, and NFC Common Access Card authentication. Physical button controls ensure that audio and video are only enabled when expressly allowed, and advanced high-assurance/common criteria EAL-2+ compliance protects against cross-network leaks.

Security runs deep, with multilayered active anti-tamper defences that instantly disable the unit if breached, while passive tamper seals provide visible intrusion detection. Versatile DisplayPort/HDMI combo connectors, USB-C variants, and legacy-compatible cables simplify deployment, and the optional SKVM Remote Control with Integrated Keyboard mirrors front-panel status via colour-coded LED backlighting, enhancing operator awareness.

SECURE DOCKING: WITHOUT THE FIRMWARE RISK

Designed as the perfect companion to Belkin Secure KVMs, the new Trade Agreement Act–compliant dock offers built-in cables and fewer ports, boosting security without sacrificing compatibility. A single USB-C cable connects the host to a clean, clutter-free workspace. Integrated ethernet switching lets two hosts share a single network connection, reducing hardware needs and deployment complexity.

Unlike aftermarket docks, the Belkin solution eliminates firmware update risks, supports up to 4K at 60 hertz video, delivers up to 100-watt pass-through power, and carries a three-year warranty. By combining robust capabilities with a minimalist design, it lowers total cost of ownership, improves reliability, and ensures compliance in high-security environments.

ONE-WAY ONLY: THE UNIDIRECTIONAL FILE TRANSFER DEVICE

Air-gapped doesn't mean invulnerable – but it can get close. Belkin's Secure Unidirectional File Transfer Device moves files like a guarded diplomatic pouch: first from source to an encrypted internal solid state drive (SSD), then from SSD to the target – never allowing a live connection between the two.

With AES-256 encryption, USB 3.0 speeds, a built-in SD card reader, and the same multilayer tamper defences as its Secure KVM siblings, it's tailor-made for defence, intelligence, and secure field operations.

Belkin understands that when the stakes are high, there's no room for compromise, and the latest product line-up deliver streamlined security for the world's most critical networks. •

belkin

Cybersecurity

Connected. Secure. Certified.

Belkin's trusted portfolio of Secure KVMs and Peripherals protect the most critical networks, ensuring the highest standards of security and performance.

- Trusted by Defence & Intelligence Agencies
- Air-gap Network Isolation
- Common Criteria Certified

www.belkin.com/au

cybersecurity.anz@belkin.com

THE HUMAN PROTOCOL: HOW CYBER SECURITY MIGHT SAVE OUR SOULS

BY MIRELLA ZULLI

Cyber security is pushing us back into something we forgot: being human.


Mirella Zulli

We often talk about cyber security as though it's cold – systems, firewalls, frameworks and zero days. But if you take a step back, you'll notice something surprising: the deeper we go into the digital world, the more we are being asked to re-engage with something profoundly analogue: our humanness.

Multi-factor authentication is a great example. It asks for something you know, something you have, and something you are. That last one, something you are, cannot be fully coded. It's presence, tone, energy. Essence. In a world racing toward replication and artificial intelligence (AI) impersonation, it turns out the thing that can't be faked is us.

This isn't a rejection of technology – far from it. This is a recognition that the human layer is not the flaw, it's the feature. We are not here to beat tech back. We are here to remind it what it's built to serve.

THE REAL-WORLD CONNECTION IS FADING, AND IT MATTERS

We are living through a time of quiet disconnection. Across the globe, research shows that real-world interaction is in sharp decline, especially among younger generations. Social media has transformed how we communicate, but has also diluted the depth and richness of that communication. We are more connected than ever, yet often less present than we've ever been.

Increased social media use is directly linked with weakened non-verbal communication and a notable drop in face-to-face interaction across Europe, Asia, and North America, as Valkenburg et al. (2024) highlights. The shift is not just social, it's structural. Hall and Liu (2022) identified a consistent pattern of 'social displacement', where time spent online steadily replaces meaningful, in-person engagement. That digital-first default is having real psychological consequences. Winstone et al. (2021) found that adolescents are experiencing a marked decline in emotional closeness and trust, as digital interaction gradually erodes the foundations of emotional bonding.

When we stop interacting in the real world, we stop learning the social skills that only emerge through friction, nuance and missteps. We stop learning how to read the room, de-escalate with body language, and build trust with eye contact.

Cyber security may seem a world away from that, but it's not. Because when human signals become harder to detect, threat surfaces expand. When the machines can mimic our voices, our faces and even our emotions, the only real security is authenticity – the kind that can't be downloaded.

RISK IS DISAPPEARING, TOO

Another layer is vanishing, and it's just as vital. Children learn to assess risk by climbing trees, arguing in the sandpit and navigating friendship breakdowns on the school oval. They learn how far to push their body, how to negotiate and how to recover from a fall. These are not just childhood memories, they are training grounds for risk literacy – the same instincts that later help us to detect danger, feel discomfort and assess trustworthiness.

Loebach et al. (2023) showed that outdoor, risk-based play does more than build physical skills; it strengthens decision-making and situational awareness. Down et al. (2024) took it further, studying teens in outdoor adventure programs, and found that managed exposure to risk fosters emotional resilience, peer trust and a sense of responsibility.

Yet, fewer children are climbing trees and fewer teenagers are being nudged towards healthy risk. What we see, instead, are rising rates of anxiety, social

fragility and a growing discomfort with uncertainty. That's not just a parenting issue, it's a security one. Because when people lose the ability to assess risk, they become easier to manipulate, exploit and deceive.

CYBER SECURITY HAS NEVER JUST BEEN ABOUT CODE

We often treat cyber security as though it is purely technical, but the truth is this: at its core, cyber security has always been about protecting people. Systems matter, but only because people rely on them. Data matters, but only because it's tied to real lives.

When we ask someone to verify their identity, we aren't just checking a login. We're asking, 'Can we trust you?' Increasingly, that answer requires more than a password – it requires presence.

The move back towards face-to-face verification, behavioural biometrics and real-world trust signals is not regression, it's restoration. It's the recognition that in a world of deepfakes, the deepest form of verification is still gut instinct.

TECHNOLOGY ISN'T THE ENEMY – IT'S THE MIRROR

Let's be clear: this isn't a tech-bashing article. I'm not here longing for a butter churner and handwritten telegrams. I like my washing machine. I love using GPS. AI is giving us all extra IQ. Technology is brilliant! It's what we let go of in the name of convenience that needs attention.

Tech isn't the villain, but it is the mirror. What it's reflecting back is that we may have digitised ourselves too far, too fast. The rise of AI and synthetic interactions is not the end of humanity. It is, in fact, a call back to it.

In a recent analysis, Mo Gawdat described AI as 'a super-intelligent child in need of careful raising', a reflection of ourselves rather than some alien threat. His metaphor reinforces that technology only magnifies what we feed it – our values, biases and attention.

Cyber security, of all things, is beginning to lead that call. It is reminding us that the strongest defence we have is not an algorithm – it's human.

REBUILDING THE VILLAGE, DIGITALLY AND LOCALLY

Our world expanded rapidly, but maybe it needs to shrink again, just a little. Children who come with their parents to the supermarket are watching micro-manners in action. They see how adults greet familiar faces, how discomfort or trust registers in body language, and how small talk turns into community. They are downloading the human protocol. When they're holding a device instead, watching *Bluey* (no shade – she's a queen!) or playing a game, they're missing all of it.

The 'village', once dissolved by speed and convenience, is still our best survival tool. Familiarity is protection. Presence is security. The human signal – flawed, beautiful and impossible to clone – is our firewall.

THE FUTURE IS HUMAN

Maybe cyber security is more than just a defence mechanism. Maybe it is the field that reminds us of what really matters – identity is more than credentials, trust can't be spoofed, and sometimes the most revolutionary thing we can do is be present.

The goal isn't to undo our progress; it's to evolve wisely. We are not here to retreat from technology, but to shape it in elegant ways that serve us and keep us stunningly human.

Because in the end, cyber security has never just been about protecting data. It's always been about protecting each other. ●

Mirella Zulli is a former teacher with 25 years of classroom experience who is now focused on uplifting cyber security awareness and training across the education and public-service sectors. Currently completing a Graduate Certificate in Cybersecurity, Zulli brings a practical, people-first approach to digital safety, combining deep pedagogical knowledge with emerging cyber capability. As a member of the Australian Women in Security Network, she's found powerful support in community-driven learning and is passionate about making cyber security accessible, relevant, and real for all learners.

References

Down, M. J. A., Picknoll, D., Edwards, T., Farringdon, F., Hoyne, G., Piggott, B., & Murphy, M. C. (2024). 'Outdoor adventure education for adolescent social and emotional wellbeing: a systematic review and meta-analysis'. Journal of Adventure Education and Outdoor Learning, *1–30. https://doi.org/10.1080/14729679.2024.2386350*

Hall, J. A., & Liu, D. (2022). 'Social media use, social displacement, and well-being'. Current Opinion in Psychology, *46, 101339. https://doi.org/10.1016/j.copsyc.2022.101339*

Loebach, J., Ramsden, R., Cox, A., Joyce, K., & Brussoni, M. (2023). 'Running the risk: The social, behavioral and environmental associations with positive risk in children's play activities in outdoor playspaces'. Journal of Outdoor and Environmental Education, *26(3), 307–339. https://doi.org/10.1007/s42322-023-00145-1*

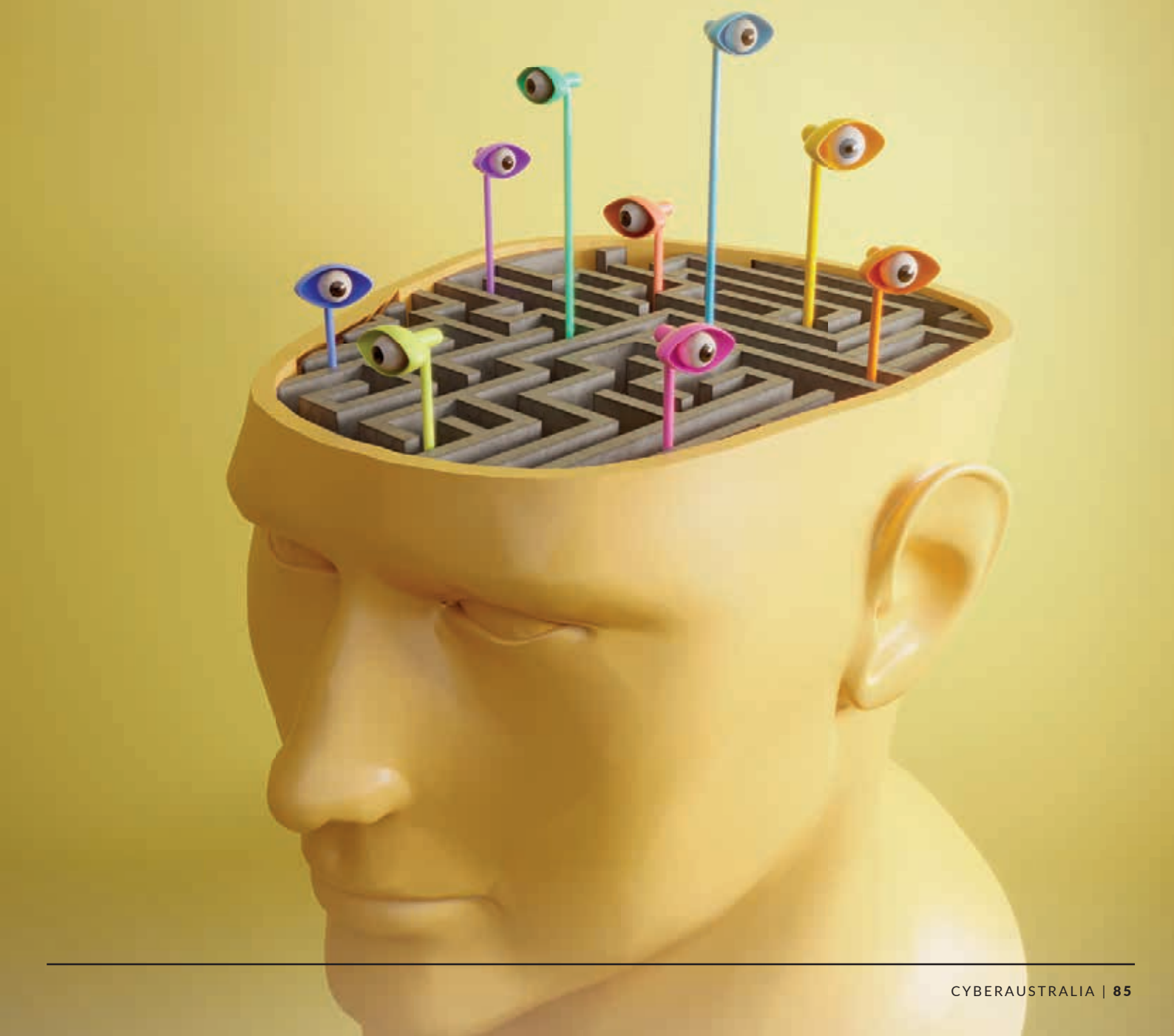
Valkenburg, P. M., Meier, A., & Beyens, I. (2022). 'Social media use and its impact on adolescent mental health: An umbrella review of the evidence'. Current Opinion in Psychology, *44, 58–68. https://doi.org/10.1016/j.copsyc.2021.08.017*

Winstone, L., Mars, B., Haworth, C. M. A., & Kidger, J. (2021). 'Social media use and social connectedness among adolescents in the United Kingdom: a qualitative exploration of displacement and stimulation'. BMC Public Health, *21(1), 1–1736. https://doi.org/10.1186/s12889-021-11802-9*

PRACTICAL ACTIONS TO SUPPORT NEURODIVERGENT MINDS IN CYBER

BY DAN MASLIN, GROUP CISO AND HEAD OF INFRASTRUCTURE STRATEGY, MONASH UNIVERSITY

Tips for cyber leaders to support a neurodivergent workforce.



Neurodivergent professionals are everywhere in cyber security – often undiagnosed, sometimes misunderstood and frequently overextended.

We don't talk about this enough – not in leadership forums, not in performance reviews, and certainly not in most team meetings – but we should. Neurodivergent people are not only over-represented in cyber; they are essential to its success.

The statistics make this clear:

- Between 20 and 30 per cent of cyber security professionals exhibit autistic traits, compared with 1–2 per cent of the general population (CREST Neurodiversity Report).
- Neurodiverse teams can outperform neurotypical teams in technical problem-solving by up to 30 per cent (CREST Neurodiversity Report).
- JPMorgan Chase's Autism at Work initiative found autistic employees were 90–140 per cent more productive than their neurotypical peers.

Cyber security attracts neurodivergent minds – and often depends on them. Deep focus, pattern recognition, relentless curiosity – these are strengths. But in the wrong environment, they are misunderstood. People get labelled as 'difficult', 'not a team player' or 'not the right fit'.

Many high-performing neurodivergent professionals are already masking daily, spending energy just to appear 'normal'. Over time, they disengage, burn out or walk away entirely. Supporting them is not only a matter of culture, but is also critical to retention and performance.

So, what can leaders do? The following are three areas where practical, evidence-based changes can make a difference.

1. STRUCTURE COMMUNICATION CLEARLY

Clear, direct communication reduces ambiguity, overthinking and anxiety. This isn't about simplifying complex ideas – it's about removing friction so people can focus on their work.

Practical steps include:

- Always provide a clear agenda for meetings – include who's attending, topics, outcomes expected and preparation needed.
- Avoid unnecessary meetings – consider written updates where suitable.
- Provide advance notice for schedule changes – last-minute surprises increase stress.
- Use detailed calendar invites with reminders – not everyone tracks time in the same way.
- Offer multiple channels – some may prefer Slack or email over live meetings.
- Provide asynchronous options – not everyone thinks best on the spot.
- Be explicit with feedback – especially about tone. For example: 'You're not in trouble. I just have five points to walk through on the report.'
- Respect social preferences – let people opt out of social events without judgement.
- Ask team members how they prefer to receive feedback – written, verbal, real-time or scheduled.

Dan Maslin

One simple tool is the 'What? By when? Why?' framework for all requests. It creates clarity and reduces stress. For example:

- **What:** 'Please review this incident report and suggest changes.'
- **By when:** 'Have this back by Friday morning.'
- **Why:** 'It needs review before I finalise for the committee Thursday afternoon.'

2. FIX THE ENVIRONMENT, NOT THE PERSON

The workplace environment determines whether people thrive or shut down. Leaders can remove barriers by making small but significant adjustments.

Practical steps include:

- Offer permanent desks rather than hot-desking – familiarity helps.
- Designate admin-only, no-meeting times for deep work.
- Provide quiet rooms, noise-cancelling headphones and adjustable lighting.
- Allow seating away from high-traffic or overstimulating areas.
- Offer ergonomic or alternative seating, such as standing desks.
- Permit sunglasses, hats or earplugs where useful.
- Provide stim tools (fidget toys, stress balls, snacks) without judgement.
- Allow flexibility in dress codes – some fabrics are intolerable for sensory reasons.
- Make space for alternative meeting styles – side-by-side laptop sessions, outdoor walks or camera-off calls.
- Encourage regular sensory breaks without requiring justification.
- Avoid strong scents – fragrance-free policies can make a difference.

If you are ever unsure, the rule is simple: choose kindness. If a tool or adjustment helps someone to manage energy, focus or wellbeing, let them use it.

3. BUILD SYSTEMS THAT WORK FOR DIFFERENCE

Neurodivergent professionals often need clear structures that reduce barriers. Leaders can rethink existing norms to enable this.

Practical steps include:

- Avoid 'culture fit' as a hiring or promotion filter – it penalises difference.
- Focus on outcomes rather than methods – different paths can still lead to excellent results.
- Challenge presenteeism – visibility is not the same as value.
- Allow flexible hours – energy levels differ, and 9 to 5 doesn't suit everyone.
- Use mini-deadlines to help with motivation, especially for ADHD. This is not about laziness – urgent or novel tasks trigger action, routine tasks often do not.
- Offer hybrid or remote set-ups where they support focus.
- Respect varied ways of contributing – silence in a meeting doesn't mean disengagement.
- Provide autonomy where possible – some thrive when trusted to lead their own process.
- Be explicit about what success looks like – don't expect people to infer unspoken rules.
- Create room for unmasking – long-term masking leads to burnout. Environments must feel safe enough for authenticity.
- Use strengths-based feedback – reinforce what's working, not just what needs 'fixing'.

A neurodivergent team member might not network widely, play politics or follow 'the usual way' – but they may be the most focused, creative or resilient person on the team.

FINAL THOUGHTS

The best teams in cyber aren't the ones where everyone thinks alike; they are the ones where difference is respected, structured and supported.

Neurodivergence should not be seen as a problem to be managed, but rather as a strength to be harnessed. A little neurodiversity makes teams more interesting – and more effective.

If you are leading a cyber team today, chances are you already have neurodivergent professionals on it. The real question is: Are they simply surviving, or are they thriving? ●

QUICK TIPS FOR LEADERS: SUPPORTING NEURODIVERGENT TALENT

- **Communicate with clarity:** Always include agendas, outcomes and timelines. Offer multiple channels and allow asynchronous responses.
- **Design the environment:** Provide quiet spaces, sensory-friendly options and predictable work settings. Avoid hot-desking if possible.
- **Be flexible:** Focus on results, not presenteeism. Allow flexible hours and hybrid arrangements where it helps.
- **Respect preferences:** Ask how people want feedback, participation and recognition. Don't judge by social events or meeting contributions alone.
- **Encourage authenticity:** Create space where masking isn't required. Support people to work in ways that align with their strengths. ●

Redefining cyber security with application control

ENTERPRISE CYBER SECURITY has long revolved around threat detection: building a perimeter around the network and trying to catch intruders before they cause too much damage. But that defensive approach has never been particularly effective, and it's far less so in today's threat landscape.

The pace and sophistication of criminal groups make Zero Trust essential: people and tools get only what they need, continuously verified. A crucial piece of that framework is controlling what applications can run and what they are allowed to do.

ThreatLocker® addresses this with Application Control, a bundle that combines Application Allowlisting and Ringfencing™ to decide what can run and to limit what approved software can do. Application Allowlisting enforces default deny so that only approved software launches, while Ringfencing limits what those approved applications can access or execute.

According to Danny Jenkins, CEO and Co-founder of ThreatLocker – a Zero Trust cyber security firm – application-focused security has become increasingly important with the explosion of tools that companies now have and make available to their employees.

'Instead of figuring out everything that's bad in the world and trying to stop it, we figure out what applications you need for your business and then block everything else by default,' Jenkins says. 'We'll also limit what those applications can do, which is what you need to prevent the fileless attacks that have become so rampant.'

Still, approved applications should not run unchecked.

'Most people don't realise that they sometimes have 500 or more applications that their computer can run,' Jenkins continues. 'Every one of those applications can see all of your files, and opens the doors to a security risk.'

This problem triggered the innovation of Ringfencing, which controls what apps can access and how they interact with other system components.

Ringfencing has helped many companies to avoid falling victim to widespread ransomware attacks by automatically denying the misuse of applications. It does this by limiting what individual programs can access. For example, as Jenkins explains, it can block them from accessing the internet or browser applications, effectively preventing them from downloading the intended malware. It also blocks unapproved executables and scripts outright, preventing unknown or malicious software from running. According to ThreatLocker, its solution has been found to reduce the time companies spend on endpoint security by 25 per cent, and allows them to re-evaluate their spending on endpoint detection and response tools.

Jenkins says that companies still need threat endpoint detection and response; but on its own, it's not enough.

'There's no point in buying 10 burglar alarms for your house and then not locking the front door,' he says. 'That's what companies need to be thinking about: they need to put a lock on their front door – and it needs to be a steel door.' ●

Not all application control is created equal.

It's time for a better way

Most solutions stop short of true protection.
ThreatLocker® delivers a Zero Trust approach that puts you in control.

- **Application Allowlisting**
  Only approved apps run. Everything else is blocked on the spot.
- **Ringfencing™**
  Limit what applications can do by locking them to only what they need to get the job done.
- **Elevation Control**
  Stop privilege exploits. Give admin rights to apps, not people.
- **10,000+ pre-built definitions**
  Easy deployment—no fuss and no disruptions.

Learn firsthand how. Request your demo today.

Contact us to get started.

THREATLOCKER®

Strengthening cyber security through inclusion

Victoria's technology workforce boasts more than 306,000 employees, yet women make up less than a third – just 29 per cent. In the field of cyber security, that figure drops even further to 17 per cent nationally. As cyberthreats continue to grow in scale and complexity, the demand for diverse perspectives and skilled talent is becoming increasingly critical. Encouraging more women to enter cyber security is not only vital for expanding the state's tech talent pool, but it also strengthens business resilience and benefits the broader community.

According to the Australian Computer Society's 2025 Digital Pulse report, the rising demand for cyber security expertise across the country is fuelling a significant talent shortage. By 2030, Australia is projected to face a shortfall of more than 54,000 skilled cyber security professionals. The report notes that a key strategy to address this shortfall is incentives to attract talent.

One program tackling this challenge head-on is Victoria's innovative Summer of Cyber Program. Designed to address gender disparity and broaden the tech talent pipeline, it's demonstrating that when women are empowered with the skills and support to thrive, the impact goes far beyond individual success – our collective cyber security becomes stronger.

This Australian-first program, launched last year, aims to give women and gender-diverse tertiary students and recent graduates valuable work experience, while also bridging the cyber skills gap and boosting cyber capability for small and medium-sized enterprises (SMEs).

The concept is simple and delivers powerful results. Through a paid studentship, students are matched with a business and gain valuable hands-on experience that strengthens their skills and boosts their job prospects. There are also significant benefits for host businesses, with no cost to participate. Hosting a student supports businesses to gain fresh perspectives and develop their workforce, as well as to solve real-world cyber challenges.

The Summer of Cyber Program is funded by the Victorian Government through the Department of Jobs, Skills, Industry and Regions, and delivered in partnership with the Australian Women in Security Network (AWSN). Summer of Cyber is one of several Victorian Government initiatives addressing the gender disparity in the digital technology workforce, and growing Victoria's digital tech capacity.

Minister for Economic Growth and Jobs Danny Pearson says the government is backing a range of programs to strengthen the state's cyber economy by getting more women skilled up to join the sector.

'More women working in cyber security is growing the sector and making it more diverse – helping us on our road to creating a cyber safe Victoria,' he says.

'Victoria's thriving tech sector contributes more than $34 billion to the state's economy, and supports

more than 306,000 workers, and the Summer of Cyber Program can help us grow this workforce even further.'

AWSN Executive Director Jacqui Loustau says the chance to partner with the Victorian Government on the program combined two of her passions – tackling the crippling effects of digital-enabled fraud on SMEs, and addressing the lack of experience that is holding talented women back in cyber security.

'When the opportunity to submit a proposal for the Summer of Cyber Program arose, AWSN jumped at it. We saw this as an innovative way to address not only the cyber security skills gap and upskill our workforce on security, but to also provide much-needed assistance to small to medium-sized Victorian businesses and startups to boost their cyber capacity,' she says.

'It helped regional students connect with regional small businesses. It helped tertiary institutions connect with industry, and helped Australia-based sovereign startups gain useful insights to improving their small business security products/services.'

'Victoria's thriving tech sector contributes more than $34 billion to the state's economy, and supports more than 306,000 workers, and the Summer of Cyber Program can help us grow this workforce even further'

Over last summer, the program matched 44 women and gender-diverse tertiary students and recent graduates with 22 Victorian SMEs. Both participants and businesses found the benefits flowed both ways – all of the students said that being part of the program boosted their confidence in their technical skills and soft skills; and businesses reported that their cyber readiness was enhanced through the program, and policies and procedures were developed and implemented.

One business that participated was Cyberoo, a leader in combating cybercrime with generative artificial intelligence (GenAI), providing solutions for both enterprises and the public to protect against scams, fraud, and online threats. Its flagship service, NothingPhishy™, delivers comprehensive digital risk protection by combining continuous monitoring, advanced threat intelligence, and GenAI with proven disruption and take-down techniques.

The project undertaken by the students involved creating a whitelist for Australia's top 100 brands – a critical step to support the company's service development. The student project supported the development of one of Cyberoo's consumer-focused platform – Scams.Report, which provides a free public service for scam verification and reporting powered by large language models. The task involved creating a whitelist for Australia's top 100 brands – a critical step to support the SME's service development.

Cyberoo's Head of Product, Sherry Wu, says the task required meticulous research and careful vetting, coupled with the need for agile decision-making, robust process management, and innovative problem-solving to effectively address the dynamic requirements facing the business.

'The implementation of the whitelist delivered significant business outcomes by establishing a trusted repository of safe websites, emails and domains. This meant we could more quickly identify suspicious activities – any data not on the whitelist was promptly flagged for deeper review – which improved scam detection and streamlined the overall verification process,' she says.

'As a result, our platform has become more reliable for users reporting potential scams. Additionally, the development process uncovered important insights: for every reputable website, there were thousands of scams, and many phishing domains cleverly mimicked verified sites by substituting even a single character from another alphabet.

'These findings further validate the strategic value of a robust, meticulously managed whitelist in bolstering cyber security.'

Deakin University student Kerry Farrea participated in the 2024–25 program. Now graduated, she says Summer of Cyber was a highlight in her cyber security journey.

'Being involved in the program gave me more than just industry experience. I worked on compliance strategy, technical content, and risk posture for responsible AI and enterprise-level privacy, but the real impact came from the support network and encouragement to lead,' she says.

'The support provided by AWSN helped me speak up with ideas that shaped discussions, grow my skills for future-ready roles, and see firsthand how representation brings better solutions.'

Her advice to other students is simple: 'Programs like this matter, and I encourage women to take part because diverse perspectives make the entire field stronger.'

The first round of the program received a ringing endorsement from all involved. As a result of this initial success, the program will run again over the coming summer, matching around 50 women and gender-diverse students or recent graduates with around 24 businesses. ●

For more information, visit www.awsn.org.au/initiatives/summer-of-cyber-program-/

AISA

Cyber | smart · safe · secure

aisa.org.au

cyber voices

THE OFFICIAL AISA PODCAST

Celebrating the diverse voices of the Australian cyber community.

DEAKIN CYBER
RESEARCH AND INNOVATION CENTRE

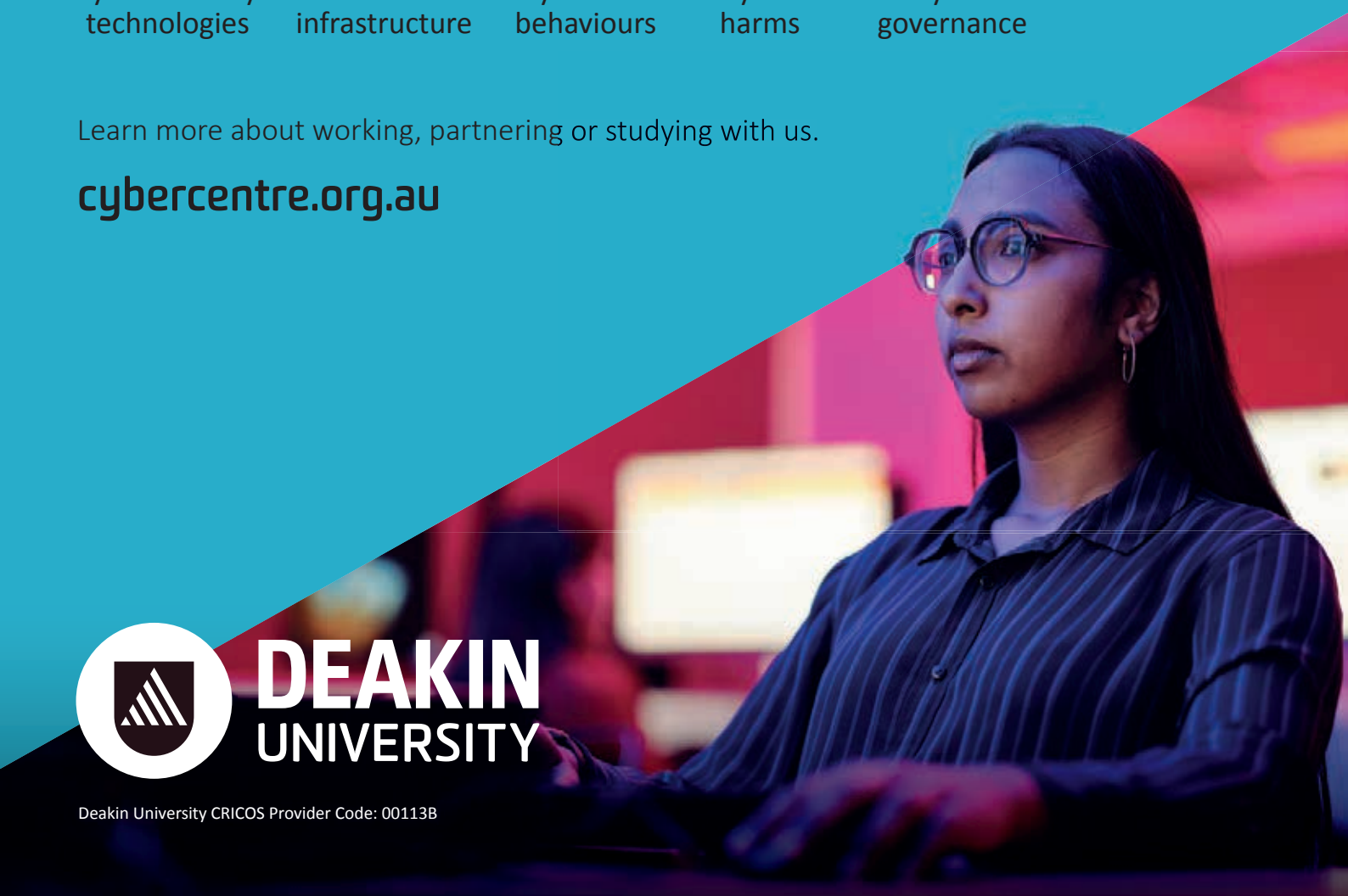
At the forefront of the changing cyber security threat landscape

We advance cyber resilience and trust to enable a thriving digital society.

- Advancing cyber security technologies
- Securing data and infrastructure
- Promoting cybersafe behaviours
- Disrupting cyber harms
- Harmonising cyber governance

Learn more about working, partnering or studying with us.

cybercentre.org.au



DEAKIN UNIVERSITY